Facultad
de
Ciencias

CUERPOS ORDENADOS
(Ordered Fields)

Trabajo de Fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Midwar Eduardo López Huapaya

Director: Luis Felipe Tabera Alonso

Diciembre - 2018

Resumen

Esta memoria recoge un estudio de los cuerpos ordenados, ordenables y formalmente reales. También se estudian los cuerpos reales cerrados, un caso particular de los cuerpos ordenados. Uno de los propósitos del trabajo es encontrar similitudes entre los cuerpos reales cerrados y el cuerpo de los números reales.

Se construye la clausura real de un cuerpo ordenado y se estudian algunas de sus características. Por último, se demuestra una caracterización de los cuerpos reales cerrados dada por Artin y Schreier.

Palabras clave: Cuerpo ordenado, Cono positivo, Cuerpo real cerrado, Clausura real, Teorema de Artin-Schreier.

Abstract

This report is focused on the study of ordered, orderable and formally real fields. Real closed fields, a particular case of ordered fields, are studied. One purpose of this work is to discuss similarities between real closed fields and the field of real numbers.

The real closure of a ordered field is built. Finally, the report concludes with a proof of a characterization of real closed fields, given by Artin and Schreier.

Key words: Ordered field, Positive cone, Real closed field, Real closure, Artin-Schreier's theorem.

Dedicado a
las personas que aguardaban este trabajo

Índice general

Introducción

El cuerpo $\mathbb{R}$ se define como el único cuerpo ordenado, arquimediano y completo. Una propiedad fundamental de $\mathbb{R}$ es que todo conjunto acotado superiormente tiene supremo. El orden nos define la topología usual, con la cual se cumplen teoremas como el del Valor Intermedio o el de Rolle. Propiedades más algebraicas pueden ser que los únicos polinomios irreducibles de $\mathbb{R}[x]$ tienen grado 1 o 2 debido a que $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ es algebraicamente cerrado, o que un elemento es mayor o igual que cero si y sólo si es un cuadrado.

En este trabajo estudiaremos los cuerpos ordenados, es decir, cuerpos en los cuales está definida una relación de orden total y compatible con la suma y el producto. Un ejemplo de cuerpo ordenado es $\mathbb{Q}$, donde está definido el orden usual. Por el contrario, el cuerpo de los números complejos $\mathbb{C}$ carece de un orden compatible con las operaciones de suma y producto. Los cuerpos de característica positiva tampoco admiten un orden. No debería resultar extraño que no se pueda definir un orden en característica positiva, debido a que no puede ocurrir que $0 < 1 < 1 + 1 < 1 + 1 + \ldots < 0$.

Primero, compararemos los conceptos de cuerpo ordenado, cuerpo ordenable y cuerpo formalmente real. Analizaremos los distintos órdenes que admite un cuerpo y los relacionaremos con los conos positivos del cuerpo (Definición 1.3) y las sumas de cuadrados.

En el segundo capítulo estudiaremos los cuerpos reales cerrados, cuerpos ordenados en los cuales todo elemento positivo posee una raíz cuadrada y todo polinomio de grado impar tiene una raíz en el cuerpo. A partir de esta definición, podemos probar que un cuerpo real cerrado R comparte muchas propiedades con $\mathbb{R}$. Tales como el Teorema del Valor Intermedio para polinomios, que $R(\sqrt{-1})$ es algebraicamente cerrado o que se cumpla el Teorema de Sturm para el conteo de raíces en un intervalo. Además, veremos algunas caracterizaciones de un cuerpo real cerrado.

En el siguiente capítulo introduciremos la noción de clausura real. Para cualquier cuerpo ordenado R, esta clausura se trata de una extensión algebraica que es real cerrado y además conserva el orden de R. Se probará además la unicidad, salvo isomorfismo, de esta clausura.

Por último, se demostrará un resultado dado por los matemáticos Emil Artin y Otto Schreier, una caracterización de los cuerpos reales cerrados. Este resultado tiene cierta belleza dentro del Álgebra, debido a que caracteriza de una forma muy general (y básica al mismo tiempo) a los cuerpos reales cerrados.

Teorema 4.1 (Teorema de Artin-Schreier) *Sea C un cuerpo algebraicamente cerrado. Si R es un subcuerpo propio de C con $[C : R]$ finito, entonces R es real cerrado y $C = R(i)$.*

Respecto al desarrollo para este trabajo, se ha de decir que se hace uso de la teoría de Galois y, por tanto, de la teoría de grupos; en particular, del Primer Teorema de Sylow, cuya demostración está incluida en el Apéndice A. También se ha de mencionar que la referencia principal de este trabajo han sido los clásicos libros "Basic Algebra"de Nathan Jacobson. Partiendo de ahí, hemos reestructurado la introducción de los conceptos, incluido ejemplos y completado las demostraciones.

Capítulo 1

Cuerpos Ordenados

Definición 1.1. *Diremos que un cuerpo R es* ***totalmente ordenado*** *(o tan sólo ordenado) si en él está definida una relación de orden $\leq$ y, además, para cualesquiera $a, b \in R$, se cumple lo siguiente:*

- *$\leq$ es total: $a \leq b$ o $b \leq a$.*
- *$\leq$ es compatible con la suma y el producto:*
  - *Si $a \leq b$ entonces $a + c \leq b + c$ para cualquier $c \in R$.*
  - *Si $a \leq b$ entonces $ac \leq bc$ para cualquier $0 \leq c$.*

Denotaremos por $(R, \leq)$ a un cuerpo ordenado R con relación de orden total $\leq$. Diremos que un cuerpo es ***ordenable*** *si es posible definir en él una relación de orden total y compatible con la suma y el producto.*

Dado un cuerpo, nos referiremos por relación de orden a una relación de orden total y compatible con la suma y el producto.

Ejemplo 1.2. *El cuerpo de los números racionales y el cuerpo de los números reales, $\mathbb{Q}$ y $\mathbb{R}$ respectivamente, son totalmente ordenados con la relación de orden usual.*

Como es usual, escribiremos $a < b$ para referirnos a que $a \leq b$, con a y b distintos. A aquellos elementos que cumplan $0 < a$ ($a < 0$) los llamaremos elementos positivos (negativos). De igual manera, diremos que un elemento no nulo tiene signo positivo o negativo. Otras veces, también podemos escribir $a \geq b$ para referirnos a $b \leq a$. También utilizaremos otra notación muy familiarizada: diremos que $x \in (a, b)$ si se cumple que $a < x < b$. Asimismo se usará la notación conocida para intervalos cerrados e intervalos semiabiertos.

En cualquier cuerpo totalmente ordenado se cumple que si $0 < a$, entonces $-a < 0$, debido a que $\leq$ es compatible con la suma. Con esto, también se cumple que si $a < b$, entonces $-b < -a$. Otra propiedad de todo cuerpo ordenado es que siempre $\mathbf{0} < \mathbf{1}$. Si tuviésemos lo contrario, también tendríamos que $0 < -1$. Y como $\leq$ es compatible con el producto, $0 \cdot (-1) < (-1) \cdot (-1)$

y con ello $0 < 1$; lo que es absurdo con lo que hemos supuesto. Ahora, como $aa^{-1} = 1 > 0$, para cualquier a no nulo, a y a^{-1} tienen el mismo signo. Si a es un elemento positivo, $(-a)^{-1} = (-1)^{-1}(a)^{-1} = -a^{-1}$.

También podemos definir el valor absoluto, $|a|$, como el máximo entre a y $-a$. Tal y como ocurre en el cuerpo $\mathbb{R}$, el valor absoluto también es siempre no negativo y además, se cumplen muchas otras propiedades, como por ejemplo: $|a + b| \leq |a| + |b|$ o $|a \cdot b| = |a||b|$.

Ahora introduzcamos una noción, en principio, distinta a la de cuerpo ordenado.

Definición 1.3. *Dado cualquier cuerpo R, un subconjunto $P \subseteq R$ se dice que es un **cono positivo** de R si cumple lo siguiente:*

- $0 \notin P$.
- *P es cerrado para la suma y el producto, es decir, si $a, b \in P$, entonces $a + b$, $ab \in P$.*
- *Si a es un elemento no nulo de R, o bien $a \in P$ o bien $-a \in P$. Es decir, R se puede escribir como unión disjunta: $-P \cup \{0\} \cup P$,*

donde $-P$ se refiere al subconjunto $\{a \in R : -a \in P\}$.

Denotaremos por (R, P) a un cuerpo R con cono positivo P.

Ejemplo 1.4. *Se puede definir un cono positivo en $\mathbb{R}$ y $\mathbb{Q}$. Este cono positivo es $P = \{x : x > 0\}$ en ambos casos, donde $>$ es la relación de orden usual.*

Sea R un cuerpo con cono positivo P. El conjunto $-P$ es cerrado para la suma, pero no para el producto. Dados $a, b \in P$, $-a + (-b) = -(a + b) \in -P$, pero $(-a)(-b) = ab \notin -P$. Por otra parte, como P sí es cerrado para el producto, para cada $a \in R$ no nulo, $a^2 \in P$. Es decir, todos los elementos cuadrados no nulos de R están en P. En particular, $1 = 1^2 \in P$.

A partir de que P es cerrado para la suma, cualquier suma finita de elementos cuadrados no nulos de R está en P. Es decir, dados unos elementos $a_1, a_2, ..., a_n$ de R no nulos, $\sum a_i^2 \in P$. En particular, $1+1+\ldots+1 \in P$ y nunca se anula. Por tanto, **todo cuerpo con cono positivo tiene característica** 0.

Además, dado que $-1 \notin P$, no es posible encontrar una raíz cuadrada de -1 en cualquier cuerpo con cono positivo, ya que entonces -1 estaría en P. Por ello, **no es posible definir un cono positivo en un cuerpo que contiene una raíz cuadrada de** -1. En particular, el cuerpo de los números complejos, $\mathbb{C}$, no posee ningún cono positivo.

Teorema 1.5. *Un cuerpo es ordenable si y sólo si tiene un cono positivo.*

Demostración. Sea $(R, \leq)$ un cuerpo ordenado. Veamos que el conjunto $P = \{a \in R : 0 < a\}$ cumple las condiciones para ser cono positivo de R:

- $0 \notin P$, debido a que $0 \not< 0$.
- P es cerrado para la suma y el producto. Sean $a, b \in P$:
  - Dado que $0 < a$ y $\leq$ es compatible con la suma, $0 + b < a + b$. Como $0 < b$ y $b < a + b$, por la propiedad transitiva de $\leq$, $0 \leq a + b$. No puede ocurrir que $a+b$ sea 0; si fuese así, como $0 < b$ y $b < a+b$, por la propiedad antisimétrica de $\leq$, b tendría que ser 0. Como $0 < b$, concluimos que $a + b \in P$.
  - A partir de que $0 < a, b$ y $\leq$ es compatible con el producto, $0 \leq ab$. Como R es cuerpo, y en particular dominio, $ab \neq 0$. Llegamos a que $ab \in P$.
- Sea a un elemento no nulo de R. Como $\leq$ es total, a es mayor o menor que 0. Por tanto, $a \in P \vee a \in -P$. Si tuviésemos que $a \in P \cap -P$, también tendríamos que $-a \in P$. Como P es cerrado para la suma, $0 = a + (-a)$ tendría que pertenecer a P, pero ya hemos visto que no puede ocurrir. Por tanto, se cumple la unión disjunta: $R = -P \cup \{0\} \cup P$.

Supongamos ahora, que R es un cuerpo con cono positivo P. Definimos la siguiente relación $\leq$:

$$a \leq b \iff (a = b \quad \vee \quad b - a \in P).$$

Veamos que esta relación es de orden. Dados $a, b, c \in R$:

- *Reflexiva*: Por la definición de $\leq$, está claro que $a \leq a$, $\forall a \in R$.
- *Transitiva*: Supongamos que $a \leq b$ y $b \leq c$. Tenemos dos casos:
  - Si $a = b$, está claro que $a \leq c$.
  - Si $b - a \in P$. Tenemos que se cumple que $c - a = (c - b) + (b - a)$. Si $b = c$, entonces $c - a = b - a$ y $a \leq c$. Si $c - b \in P$, como P es cerrado para la suma, llegamos a que $a \leq c$.
- *Antisimétrica*: Supongamos que $a \leq b$ y $b \leq a$. Si a fuese distinto de b, tendríamos que $b-a$ y $a-b$ pertenecerían a P. Y entonces $(b-a)+(a-b) = 0$ también estaría en P, lo cual es absurdo. Por tanto, $a = b$.

Ahora veamos que $\leq$ es total y compatible con la suma y el producto. Sean $a, b \in R$ cualesquiera:

- $\leq$ es total: si $a \not\leq b$, entonces $a \neq b$ y $b - a \notin P$. Como $R = -P \cup \{0\} \cup P$, $b - a \in -P$. Por tanto, $-(b - a) = a - b \in P$. Entonces, $b \leq a$.
- $\leq$ es compatible con la suma. Si $a \leq b$, entonces $b - a \in P \cup \{0\}$. Si c es cualquier elemento de R, $(b + c) - (a + c) = b - a$. Entonces $a + c \leq b + c$.

- $\leq$ es compatible con el producto. Si $a \leq b$ y $0 \leq c$, tenemos tres casos:
  - Si $a = b$, entonces $ac = bc$ y $ac \leq bc$.
  - Si $b - a \in P$ y $0 = c$, está claro que $ac \leq bc$.
  - Si $b - a \in P$ y $0 < c$. Tenemos que se cumple $bc - ac = (b - a)c$. Entonces, $bc - ac \in P$, ya que P es cerrado para el producto. Por tanto, $ac \leq bc$.

Entonces, la relación $\leq$ dota de un orden a R. □

A partir de ahora, dado que las nociones son equivalentes, nos referiremos por cuerpo ordenado tanto a un cuerpo con cono positivo, como a un cuerpo con una relación de orden. De igual manera, diremos que un cuerpo es ordenable, si en él es posible definir una relación de orden o encontrar un cono positivo. Por la misma razón, no será extraño que nos refiramos por elementos positivos tanto a los elementos mayores que 0, como a los elementos del cono positivo.

Se ha de recalcar que en ciertos cuerpos es posible definir más de un cono positivo (o ninguno). Y por ello, también es posible definir más de una relación de orden. Para ver un ejemplo de estos cuerpos, es necesario introducir la noción de orden inducido (pág. 12). Primero veamos que el **orden de $\mathbb{Q}$ es único**. Este orden será el que da la relación de orden usual, mostrada en el Ejemplo 1.4.

Ejemplo 1.6. *El signo de cualquier elemento $\frac{a}{b}$ no nulo de $\mathbb{Q}$ está determinado por el signo de $\frac{a}{1}$ y $\frac{b}{1}$; debido a que sólo así es posible que se cumpla la propiedad, de un cono positivo, de ser cerrado para el producto. Si ambos tienen el mismo signo, $\frac{a}{b}$ es positivo. En cambio, si tienen distinto signo, entonces $\frac{a}{b}$ es negativo.*

Por otra parte, cualquier elemento de $\mathbb{Q}$ de la forma $\frac{m}{1}$, $m \in \mathbb{Z}$, se puede expresar: o bien $\frac{m}{1} = 1 + \ldots + 1$, o bien $\frac{m}{1} = (-1) + \ldots + (-1)$, debido a que $\mathbb{Z} =< 1 >$ es un grupo cíclico. Por tanto, para cualquier orden, el signo de un elemento de la forma $\frac{m}{1}$ está determinado según si este es suma de 1 o de -1. De esta forma, el signo de un elemento no nulo $\frac{a}{b}$ es el mismo en todos los ordenes de $\mathbb{Q}$. Por tanto, el orden de $\mathbb{Q}$ es único.

Otra conclusión que se puede obtener a partir del Teorema 1.5 es que dada una relación de orden, existe un cono positivo asociado a esta relación. De igual manera, dado un cono positivo, existe una relación de orden asociada a este. El siguiente resultado nos muestra que el número de conos positivos que se pueden definir en un cuerpo es el mismo que el número de relaciones de orden que hacen al cuerpo ordenable. La forma en que se asocian relaciones de orden y conos positivos es la misma que en la demostración anterior.

Teorema 1.7. *Dado un cuerpo R. Existe una biyección entre los posibles conos positivos P de R, y las relaciones de orden total compatibles con la suma y el producto que pueden ser definidas en R.*

Demostración. Sea R un cuerpo. Supongamos que R contiene dos conos positivos distintos, P_1 y P_2, y que estos tienen asociada la misma relación de orden, $\leq$. Dado que los conos son distintos: o bien existe un x no nulo en $P_1 \setminus P_2$, o bien existe un x no nulo en $P_2 \setminus P_1$. Los dos casos son idénticos, veamos el primero. Como $x \in P_1$, entonces $x > 0$, y como $x \notin P_2$, entonces $x < 0$. Por la propiedad antisimétrica de $\leq$ tenemos que $x = 0$, lo que es absurdo ya que x es no nulo. Por tanto, no puede ocurrir que dos conos positivos distintos tengan la misma relación de orden asociada.

Ahora supongamos que tenemos dos relaciones de orden distintas, $\leq_1$ y $\leq_2$, y un cono positivo P asociado a estas. Como las relaciones son distintas, existe x no nulo tal que $0 \leq_1 x$ y $x \leq_2 0$. Por tanto, tenemos que $x \in P$ a la vez que $x \notin P$, lo que es absurdo. Por tanto, los conos positivos asociados de dos relaciones de orden distintas, tienen que ser distintos. □

Teorema 1.8 ([1], ejercicio 1 p. 311)**.** *Si R es un cuerpo en el cual -1 no es un cuadrado y la suma de dos cualesquiera no cuadrados es un no cuadrado, entonces R es un cuerpo ordenado.*

Demostración. Sea R un cuerpo con las condiciones anteriores. Llamemos P al conjunto de elementos cuadrados no nulos de R. Veamos que P cumple las condiciones para ser un cono positivo de R:

- $0 \notin P$ por cómo se ha definido P.

- Sea a un elemento no nulo de R. Si a es un cuadrado, entonces $a \in P$. Si a no es un cuadrado, entonces $-a$ es un cuadrado; ya que de no ser así, 0 sería un no cuadrado por ser suma de no cuadrados: $0 = a + (-a)$. Es obvio que un elemento no puede ser cuadrado y no cuadrado a la vez, por tanto, se cumple la unión disjunta: $R = -P \cup \{0\} \cup P$.

- Sean $a, b \in P$, entonces $a = m^2$ y $b = n^2$ para ciertos m, $n \in R$. Entonces $ab = (mn)^2$ y $ab \in P$. Falta ver que la suma está en P. Primero vemos que el elemento $-a$ no puede ser un cuadrado, ya que de ser así, $-1 = (-a)(a^{-1})$ sería también un cuadrado por poder expresarse como producto de cuadrados. Si $a + b$ no fuese un cuadrado, tendríamos que $(a + b) + (-a)$ sería un no cuadrado por ser suma de no cuadrados. Pero como esto es igual a b, que sí que es un cuadrado, vemos que no puede ocurrir que $a+b \notin P$. Por tanto, P es cerrado para la suma y el producto.

□

Hemos visto como algunas propiedades conocidas para $\mathbb{R}$ también se cumplen en los cuerpos ordenados. En el siguiente teorema vamos a ver un resultado muy conocido en el anillo de polinomios $\mathbb{R}[x]$, pero aplicado para cualquier cuerpo ordenado.

Teorema 1.9 ([1], ejercicio 4 p. 311)**.** *Sea $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ un polinomio mónico de $R[x]$, con R un cuerpo ordenado. Definimos $M = 1 + |a_{n-1}| + \ldots + |a_0| \in R$. Las raíces de $f(x)$ contenidas en R están en el intervalo $(-M, M)$, debido a que si $|t| > M$, entonces $|f(t)| > 0$.*

Este teorema puede ser aplicado a cualquier polinomio de $R[x]$. Dado que R es cuerpo, para cualquier polinomio $g(x) \in R[x]$, existe $r \in R$ de modo que $rg(x)$ es un polinomio mónico de $R[x]$. Como R es cuerpo, en particular dominio, $rg(x)$ tiene las mismas raíces que $g(x)$.

Demostración. Sean $f(x)$ y M como en las condiciones del teorema. Supongamos que $|t| > M$. Entonces $|t| > 1$ por como está definido M. Con esto, $|t|^j \leq |t|^{j+1}$, para cualquier $j \in \mathbb{N} \cup \{0\}$. Así, $|t|^j \leq |t|^{n-1}$ $(-|t|^j \geq -|t|^{n-1})$, para cada $0 \leq j \leq n-1$.

Para ver que $|f(t)|$ es no nulo, vamos a usar algunas propiedades del valor absoluto. Entre ellas: $|a - b| \geq |a| - |b|$. He alineado las ecuaciones.

$$\begin{aligned}
|f(t)| &= \left| t^n + \sum_{i=0}^{n-1} a_i t^i \right| = \left| t^n - \left(-\sum_{i=0}^{n-1} a_i t^i \right) \right| \geq |t^n| - \left| -\sum_{i=0}^{n-1} a_i t^i \right| \\
&= |t|^n - \left| \sum_{i=0}^{n-1} a_i t^i \right| \geq |t|^n - \sum_{i=0}^{n-1} \left| a_i t^i \right| = |t|^n - \sum_{i=0}^{n-1} |a_i||t|^i \\
&\geq |t|^n - \sum_{i=0}^{n-1} |a_i||t|^{n-1} = |t|^n - |t|^{n-1} \sum_{i=0}^{n-1} |a_i| = |t|^{n-1} \left(|t| - \sum_{i=0}^{n-1} |a_i| \right).
\end{aligned}$$

Dado que $|t| > M > \sum_{i=0}^{n-1} |a_i|$, el último término obtenido es mayor que 0. Y por tanto, hemos probado que si $|t| > M$, entonces $|f(t)| > 0$. □

Ahora, vamos a introducir la noción de orden inducido. Para ello, vemos que los subcuerpos de un cuerpo ordenado también son cuerpos ordenados:

Lema 1.10. *Sea (R, P) un cuerpo ordenado y F un subcuerpo de R. Tenemos que F es un cuerpo ordenado con cono positivo $P \cap F$.*

Demostración. Es una mera comprobación. □

Definición 1.11. *Dado un cuerpo ordenado (R, P) y F un subcuerpo de R. El orden que se define en F por el cono positivo $P' = P \cap F$ se llama* ***orden inducido*** *en F.*

Si E es un cuerpo ordenado que contiene a R, diremos que el orden de E es una ***extensión del orden*** *de R si el orden, en R, de los elementos de R se mantiene en el orden de E.*

Ejemplo 1.12. *Como todo cuerpo ordenado tiene característica 0, $\mathbb{Q}$ está contenido en todo cuerpo ordenado. Dado que $\mathbb{Q}$ tiene orden único, el orden inducido por cualquier cuerpo ordenado sobre $\mathbb{Q}$ es el mismo.*

Ejemplo 1.13 ([1], ejercicio 2 p. 311)**.** *El cuerpo $\mathbb{Q}(\sqrt{2})$ puede ordenarse de dos (y sólo dos) formas distintas. Por lo visto en el Ejemplo 1.12 anterior, cualquier orden de $\mathbb{Q}(\sqrt{2})$ es extensión del orden de $\mathbb{Q}$.*

Supongamos que tenemos una relación de orden $\leq_1$ en $\mathbb{Q}(\sqrt{2})$ y que $\sqrt{2} >_1 0$. Sea $a+b\sqrt{2}$ un elemento de $\mathbb{Q}(\sqrt{2})$. Si $a+b\sqrt{2}$ es positivo, según la relación $\leq_1$, entonces se cumple que $b\sqrt{2} >_1 -a$. Podemos separar tres casos:

- *$a = 0$. Como $\sqrt{2}$ es positivo, $b\sqrt{2} >_1 0$ si y sólo si $b >_1 0$.*
- *$a \neq 0 \wedge b >_1 0$. Dividiendo por $-b$, obtenemos $-\sqrt{2} <_1 \frac{a}{b}$. Dado que $-\sqrt{2}$ es negativo y b es positivo, esto se cumple para cualquier a positivo. Si a es negativo, sólo se cumple si $\left(\frac{a}{b}\right)^2 <_1 2$.*
- *$a \neq 0 \wedge b <_1 0$. Dividiendo por $-b$, $-\sqrt{2} >_1 \frac{a}{b}$. Como $-\sqrt{2}$ es negativo, sólo es posible que a sea positivo y se cumpla $\left(\frac{a}{b}\right)^2 >_1 2$.*

Ahora supongamos que tenemos otra relación de orden, $\leq_2$, y que, en este caso, $\sqrt{2} <_2 0$. Como antes, dado un elemento $a + b\sqrt{2}$ de $\mathbb{Q}(\sqrt{2})$, podemos ver la condiciones con las que este es positivo. Haciendo lo mismo que antes, llegamos a los mismos tres casos, pero con distintos resultados:

- *$a = 0$. Como $\sqrt{2}$ es negativo, $b\sqrt{2} >_2 0$ si y sólo si $b <_2 0$.*
- *$a \neq 0 \wedge b >_2 0$. Al igual que antes, $-\sqrt{2} <_2 \frac{a}{b}$. Como esta vez $-\sqrt{2}$ es positivo, sólo es posible si $a > 0$ y $\left(\frac{a}{b}\right)^2 >_2 2$.*
- *$a \neq 0 \wedge b <_2 0$. Entonces, dividiendo por $-b$, $-\sqrt{2} >_2 \frac{a}{b}$. Como $-\sqrt{2}$ es positivo y b negativo, se cumple siempre que a sea positivo. Si a es menor que 0, sólo se cumple si $\left(\frac{a}{b}\right)^2 <_2 2$.*

Queda ver que estas relaciones definen un orden en $\mathbb{Q}(\sqrt{2})$. La primera relación es el orden inducido por $\mathbb{R}$ y la segunda es el orden obtenido al realizar el automorfismo de $\mathbb{Q}(\sqrt{2})$, $\sqrt{2} \mapsto -\sqrt{2}$.

Definición 1.14. *Sean $E \supseteq R$ dos cuerpos ordenados donde el orden de E es una extensión del orden de R. Diremos que un elemento positivo $x \in E$ es **infinitamente pequeño (grande) sobre** R si x es menor (mayor) que cualquier elemento positivo de R.*

Está claro que si un elemento es infinitamente grande sobre un cuerpo, su inverso será infinitamente pequeño.

Dado un cuerpo ordenado R, se puede definir más de un orden en su cuerpo de funciones racionales en una variable, $R(x)$. Detallaremos uno de estos órdenes en el Teorema 1.15; y veremos que se pueden encontrar elementos infinitamente pequeños (y elementos infinitamente grandes) sobre R.

Pero antes, demos una notación que facilitará la lectura del Teorema 1.15 y su respectiva demostración. Dado un polinomio $f(x) = a_n x^n + \ldots + a_0$ no

nulo con coeficientes en R, llamaremos $sc(f(x))$ al primer a_i no nulo, empezando desde a_0. Dado que R es cuerpo, y en particular dominio, está claro que $sc(f(x)g(x)) = sc(f(x)) \cdot sc(g(x))$, para cualesquiera $f(x)$, $g(x) \in R[x]$ no nulos. Si tenemos $h(x) = \frac{f(x)}{g(x)} \in R(x)$, también denotaremos por $sc(h(x))$ al correspondiente $sc(f(x))/sc(g(x))$. En el caso de que $h(x) = 0$, tomaremos $sc(h(x)) = 0$.

Teorema 1.15 ([4], ejercicio 2.6 p. 27)**.** *Dado un cuerpo ordenado $(R, \leq_R)$, su cuerpo de funciones racionales en una variable, $R(x)$, es ordenado con la siguiente relación $\leq$:*

$$0 < h(x) \iff 0 <_R sc(h(x))$$

Demostración. Sea $S = \{h(x) \in R(x) : 0 < h(x)\}$, donde $\leq$ es la relación definida en el enunciado del teorema. Por el Teorema 1.5, si probamos que S es un cono positivo, entonces la relación $\leq$ es de orden. Por esta razón, probemos que S es un cono positivo de $R(x)$:

- $0 \notin S$ ya que $0 \not<_R 0$.
- Sea $h(x)$ un elemento no nulo de $R(x)$. Si $0 <_R sc(h(x))$, entonces $h(x) \in S$. Si $0 \not<_R sc(h(x))$, entonces $0 < -sc(h(x))$ debido a que $\leq_R$ es una relación de orden en R; con ello, $-h(x) \in S$. Por otra parte, si existe $h(x) \in -S \cap S$, entonces se tiene que $0 < h(x)$ y $0 < -h(x)$. Con esto, tendríamos que existe un elemento no nulo $sc(h(x)) = a \in R$ cumpliendo: $(0 <_R a) \wedge (0 <_R -a)$, lo que es absurdo ya que R es ordenado. Por tanto, se cumple la unión disjunta: $R(x) = -S \cup \{0\} \cup S$.
- Sean $f(x) = \frac{f_1(x)}{f_2(x)}$, $g(x) = \frac{g_1(x)}{g_2(x)}$ dos elementos de S. Llamemos a, b, c y d a los respectivos sc de f_1, f_2, g_1 y $g_2 \in R[x]$. Dado que f y g pertenecen a S, se tiene que a/b y c/d son elementos positivos de $(R, \leq_R)$.

  Tenemos que $f + g = \frac{f_1 g_2 + f_2 g_1}{f_2 g_2}$ y $sc(f + g) = sc(f_1 g_2 + f_2 g_1)/sc(f_2 g_2)$. Como $sc(f_1 g_2 + f_2 g_1) \in \{ad, bc, ad+bc\}$, $sc(f+g) \in \{a/b, c/d, a/b+c/d\}$. Dado que a/b y c/d son elementos positivos, estos tres últimos elementos también son positivos. Por ello, $sc(f + g) >_R 0$ y $f + g \in S$.

  Por último, como $fg = \frac{f_1 g_1}{f_2 g_2}$, tenemos que $sc(fg) = ac/(bd)$. Este elemento también es positivo en R, debido a que es producto de dos elementos positivos. Por tanto $fg \in S$, y S es cerrado para la suma y el producto.

□

Según como hemos definido este orden en $R(x)$, está claro que es una extensión del orden de R. Podemos encontrar elementos infinitamente pequeños sobre R. Dado que $sc(x) = 1$, x es un elemento positivo de $R(x)$. Ahora, para cualquier elemento positivo a de R, $x - a < 0$. Por tanto $x < a$, para todo

a positivo de R; y x es infinitamente pequeño sobre R. Con esto, también se tiene que x^{-1} es infinitamente grande sobre R.

Se puede ver que este es el único orden de $R(x)$ en el cual x es infinitamente pequeño sobre R. Como $x < 1$, se tiene que $0 < x^n - x^{n+1}$, para todo $n \geq 0$. Así, el orden de un polinomio de $R[x]$ estará determinado por el coeficiente no nulo más pequeño.

Por otro lado, es posible definir otro orden en $R(x)$, en el cual se tornan las situaciones entre x y x^{-1} sobre R. Para ello, al igual que hemos hecho para el Teorema 1.15, cada elemento $h(x) = \frac{f(x)}{g(x)}$ de $R(x)$ hemos de asociarlo al coeficiente director del correspondiente polinomio $f(x)g(x) \in R[x]$; lo denotamos por $lt(h(x))$. Así, la siguiente relación $\leq_n$ define un orden en $R(x)$:

$$0 <_n h(x) \iff 0 <_R lt(h(x))$$

La demostración es muy similar a la del Teorema 1.15. Además, también será el único orden de $R(x)$ en el cual x es infinitamente grande sobre R.

Por otra parte, dado un cuerpo ordenado R y un elemento trascendente sobre R, ε, como los cuerpos $R(x)$ y $R(\varepsilon)$ son isomorfos, los posibles ordenes de $R(\varepsilon)$ son los mismos ordenes de $R(x)$. Estos ordenes se trasladan mediante el isomorfismo $\varphi : \frac{f(x)}{g(x)} \mapsto \frac{f(\varepsilon)}{g(\varepsilon)}$.

Ejemplo 1.16. *Aplicando esta construcción a $\mathbb{Q}$ y al número π (trascendente sobre $\mathbb{Q}$), nos encontramos con que existe un orden en $\mathbb{Q}(\pi)$ en el cual π es infinitamente pequeño sobre $\mathbb{Q}$.*

Por otra parte, sabemos que la relación de orden usual define un orden en $\mathbb{R}$ (más adelante veremos que este orden es único en $\mathbb{R}$). Dado que $\mathbb{Q}(\pi)$ es subcuerpo de $\mathbb{R}$, podemos inducir la relación de orden usual sobre $\mathbb{Q}(\pi)$. Con esto, tenemos otro orden en $\mathbb{Q}(\pi)$ donde se cumple que $3 < \pi < 4$. Por tanto, existe un orden en $\mathbb{Q}(x)$ donde $3 < x < 4$.

Definición 1.17. *Dados dos cuerpos ordenados (R, P) y (R', P'), un homomorfismo φ entre R y R' se llama **homomorfismo ordenado** si $\varphi(P) \subseteq P'$. Si φ es un isomorfismo, diremos que es un **isomorfismo ordenado**.*

Supongamos que φ es un isomorfismo ordenado entre los cuerpos (R, P) y (R', P'). Si y es un elemento de P', sabemos que existe un (único) $x \neq 0 \in R$ tal que $\varphi(x) = y$. Si este x perteneciese a $-P$, entonces $-x \in P$ y $\varphi(-x) = -y$ pertenecería a P'. Tendríamos un elemento no nulo de R' tal que $y, -y \in P'$, lo cual es absurdo. Así, en un isomorfismo ordenado se tiene que $\varphi(P) = P'$.

Por otra parte, todo isomorfismo ordenado tiene dos propiedades interesantes para este trabajo:

- Conserva el orden: Si $a < b$, entonces $b - a > 0$ y $\varphi(b - a) > 0$. Por tanto, $\varphi(b) - \varphi(a) > 0$ y $\varphi(b) > \varphi(a)$.
- Para todo $a \in R$, $\varphi(|a|) = |\varphi(a)|$. Si $a > 0$, entonces $\varphi(|a|) = \varphi(a) > 0$ y $|\varphi(a)| = \varphi(a)$. Si $a < 0$, entonces $\varphi(|a|) = \varphi(-a) > 0$ y $|\varphi(a)| = -\varphi(a)$.

El concepto de isomorfismo ordenado será importante más adelante. Primero, veamos otra noción que está estrechamente relacionado con los cuerpos ordenados.

1.1. Cuerpos Formalmente Reales

Definición 1.18. *Un cuerpo R se dice* ***formalmente real*** *si -1 no puede escribirse como suma de elementos cuadrados de R.*

Ejemplo 1.19. *Los cuerpos $\mathbb{R}$ y $\mathbb{Q}$ son formalmente reales. De hecho, más adelante veremos que las nociones de cuerpo ordenable y cuerpo formalmente real son equivalentes. Evidentemente, cualquier cuerpo que contenga una raíz cuadrada de -1 no es formalmente real ya que $-1 = (\sqrt{-1})^2$.*

Teorema 1.20. *Un cuerpo R es formalmente real si y sólo en él se cumple: si $\sum_{i=1}^{n} a_i^2 = 0$, con $a_i \in R$, $n \in \mathbb{N}$, entonces $a_i = 0$ para cada $i = 1, \ldots, n$.*

Demostración. Supongamos que R es un cuerpo formalmente real y que existen $a_i \in R$ no nulos de modo que $a_1^2 + \ldots + a_n^2 = 0$. Multiplicando por $a_1^{-2} \in R$, $1 + (\frac{a_2}{a_1})^2 + \ldots + (\frac{a_n}{a_1})^2 = 0$. Y entonces tendríamos que -1 puede escribirse como suma de cuadrados, lo que contradice al hecho de que R es formalmente real. Por tanto, sólo es posible que cada a_i sea 0.

Ahora supongamos que R es un cuerpo en el que toda suma finita de elementos cuadrados no nulos, es distinta de cero. Si -1 es una suma de cuadrados de R, $-1 = \sum a_i^2$, encontraríamos que $0 = \sum a_i^2 + 1^2$. Como esto no puede ocurrir, R es formalmente real. □

Si R es un cuerpo no formalmente real, entonces existe un número finito de $a_i \in R$ tales que $-1 = \sum a_i^2$. Si además, la característica de R es distinta de 2, podemos asegurar que todo elemento a de R se puede escribir como suma de cuadrados:

$$a = \frac{4a}{4} = \frac{4a + (1+a^2) - (1+a^2)}{4} = \frac{2a + 1 + a^2 + 2a - 1 - a^2}{4}$$
$$= \left(\frac{1+a}{2}\right)^2 - \left(\frac{1-a}{2}\right)^2 = \left(\frac{1+a}{2}\right)^2 + \sum a_i^2 \left(\frac{1-a}{2}\right)^2.$$

Teorema 1.21. *Sea R un cuerpo de característica 0. Si existe $a \in R$ que no es suma de cuadrados, entonces R es formalmente real.*

Demostración. El contra-recíproco está probado con lo expuesto antes del enunciado. □

A continuación, vamos a ver que las nociones de cuerpo ordenable y cuerpo formalmente real son equivalentes en el Teorema 1.24. Pero antes, tendremos que suponer el Lema de Zorn:

Lema 1.22 (**Lema de Zorn**). *Sea $(M, \leq)$ un conjunto no vacío parcialmente ordenado, en el cual toda cadena tiene cota superior en M. Entonces, existe un elemento maximal en $(M, \leq)$.*

Recordemos que un conjunto parcialmente ordenado $(M, \leq)$ es un conjunto ordenado donde la relación de orden $\leq$ no tiene por qué ser total. Y una cadena es un subconjunto de M donde la relación de orden inducida por $(M, \leq)$ sí que es total.

Además del Lema de Zorn, será de gran utilidad el siguiente resultado:

Lema 1.23. *Sea F un cuerpo. Supongamos que P_0 es un subgrupo de $(F^*, \cdot)$, cerrado para la suma y que contiene a todos los elementos cuadrados no nulos de F. Si a es un elemento no nulo de F, con $-a \notin P_0$, entonces el conjunto $P_1 = \{m + an : m, n \in P_0\}$ es un subgrupo de $(F^*, \cdot)$ cerrado para la suma. Además, contiene a P_0 y a a.*

Demostración. Supongamos que estamos en las condiciones del Lema. Dado que P_0 es subgrupo de $(F^*, \cdot)$, entonces P_0 también es cerrado para el producto.

Primero veamos que $P_1 = \{m + an : m, n \in P_0\}$ es cerrado para la suma y el producto. Sean $m = m_1 + am_2$, $n = n_1 + an_2$ dos elementos cualesquiera de P_1:

- $m + n = (m_1 + n_1) + a(m_2 + n_2)$
- $mn = (m_1 n_1 + a^2 m_2 n_2) + a(m_2 n_1 + m_1 n_2)$.

Por las hipótesis de P_0, tenemos que $a^2 \in P_0$ por ser $a \neq 0$. Además, P_0 es cerrado para la suma y el producto, por lo que $m + n$ y mn pertenecen a P_1.

Ahora veamos que P_1 es subgrupo de F^*:

- $0 \notin P_1$: si esto no fuese así, tendríamos que $0 = m + an$, para ciertos $m, n \in P_0$. Con ello tendríamos que $-a = mn^{-1}$ y como P_0 es cerrado para el producto, estaríamos contradiciendo la hipótesis de $-a \notin P_0$.
- P_1 es cerrado para el producto.
- Si $m + an \in P_1$, entonces $(m + an)^{-1} \in P_1$: tenemos que $m + an \neq 0$ porque 0 no pertenece a P_1. En F, $(m + an)^{-1}$ se puede expresar de la forma: $(m + an)(m + an)^{-2} = m(m + an)^{-2} + an(m + an)^{-2}$. Debido a que P_0 es cerrado para el producto y contiene a los elementos cuadrados de F^*, $(m + an)^{-1} \in P_1$.

Por último, veamos que $P_0 \subseteq P_1$. Dado que $1 \in P_1$, existen m, $n \in P_0$ de modo que $1 = m + an$. Para cualquier $p \in P_0$, se tiene que: $p = pm + apn$. Dado que P_0 es cerrado para el producto, $p \in P_1$. Se tiene también que $a = a^2 n + am \in P_1$. □

Ahora ya podemos probar lo siguiente:

Teorema 1.24. *Un cuerpo es ordenable si y sólo si es formalmente real.*

Demostración. Supongamos que R es un cuerpo ordenable. Sabemos que en todo cuerpo ordenado, 1 es siempre positivo: por tanto, -1 no puede pertenecer al conjunto de elementos positivos. Si -1 pudiese expresarse como suma de cuadrados, entonces pertenecería al conjunto de elementos positivos, lo cual es absurdo. Por tanto, cuerpo ordenable implica cuerpo formalmente real.

Supongamos ahora que R es formalmente real. Consideremos el subconjunto de R^*: $P_0 = \{a_1^2 + \ldots + a_n^2 : a_i \in R^*, n \in \mathbb{N}\}$. Dado que R^* es no vacío, P_0 tampoco lo es. Está claro que este subconjunto es cerrado para la suma y contiene a todos los elementos cuadrados de R^*. Además, podemos ver que P_0 es subgrupo de $(R^*, \cdot)$:

- $0 \notin P_0$: dado que R es formalmente real, en el Teorema 1.20 vimos que ninguna suma finita de elementos cuadrados de R^* es igual a 0.
- P_0 es cerrado para el producto: si $\sum a_i^2$ y $\sum b_j^2$ son dos elementos de P_0, $\sum a_i^2 \sum b_j^2 = \sum (a_i b_j)^2 \in P_0$.
- Si $a = \sum a_i^2 \in P_0$, entonces $a^{-1} \in P_0$: el inverso de a (en R) puede expresarse de la forma: $a^{-1} = aa^{-2}$. Tenemos que $a \neq 0$ ya que $0 \notin P_0$; entonces a^{-2} es un cuadrado no nulo de R y pertenece a P_0. Dado que P_0 es cerrado para el producto, a^{-1} también pertenece a P_0.

Ahora llamemos $\mathcal{A}$ al conjunto de subconjuntos de R que sean subgrupo de $(R^*, \cdot)$, cerrado para la suma y que contengan a todos los elementos cuadrados no nulos de R. Este conjunto es no vacío, ya que al menos P_0 pertenece a él. Consideramos el contenido $\subseteq$ como relación de orden parcial en $\mathcal{A}$.

Sea $\{P_i\}_{i \in I}$ una cadena en $\mathcal{A}$. Por la definición de cadena, tenemos que si $i, j \in I$, entonces $P_i \subseteq P_j \vee P_j \subseteq P_i$. Veamos que el conjunto $M = \bigcup_{i \in I} P_i$ (que es una cota superior de la cadena) pertenece a $\mathcal{A}$:

- Es subgrupo de R^*:
  - $0 \notin M$ porque $0 \notin P_i, \forall i \in I$.
  - Sean $m_1 \in P_i$, $m_2 \in P_j$ elementos de M. Sabemos que o bien $P_i \subseteq P_j$, o bien $P_j \subseteq P_i$. Dado que todos los elementos de $\mathcal{A}$ son subgrupos de $(F^*, \cdot)$, $m_1 m_2^{-1} \in P_k$, para $k = i \vee k = j$. Por tanto, $m_1 m_2^{-1} \in M$.
- Podemos ver que es cerrado para la suma de la misma forma que en el punto anterior.
- Contiene a todos los elementos cuadrados de R^*, ya que todos estos están en cada P_i.

Por tanto, estamos en las condiciones para poder aplicar el Lema de Zorn, y con ello, existe al menos un elemento maximal P en $\mathcal{A}$. Podemos comprobar que este conjunto dota a nuestro cuerpo R de un orden:

- $0 \notin P$ porque 0 no pertenece a ningún elemento de $\mathcal{A}$.
- Dados $a, b \in P$, $a + b$ y $ab \in P$ ya que todos los elementos de $\mathcal{A}$ son cerrados para la suma y subgrupos de R^*.
- Queda ver si se cumpla la unión disjunta $R = -P \cup \{0\} \cup P$:
  - Supongamos que existe un elemento no nulo de R, a, que no pertenece ni a P ni a $-P$. Por el Lema 1.23 demostrado antes, existe un subgrupo de R^* de la forma $P_1 = P + aP$, cerrado para la suma y, además, se cumple que $P \subseteq P_1$. La contención es estricta; dado que P_1 es subgrupo de $(R^*, \cdot)$, existen m, $n \in P$ (no nulos) de modo que $1 = m + an$. Multiplicando por a, tenemos que $a = ma + a^2n$. Como P contiene a los elementos cuadrados de R^*, tenemos que $a \in P_1 \setminus P$. Ahora, como P está contenido en P_1, este último contiene a todos los elementos cuadrados no nulos de R. Hemos encontrado otro elemento de $\mathcal{A}$ que contiene a P estrictamente. Pero esto no puede ocurrir ya que P es un elemento maximal de $\mathcal{A}$.
    Entonces se cumple que, dado $a \in R^*$: $a \in P \vee a \in -P$.
  - Como 0 no pertenece a P, entonces 0 tampoco pertenece a $-P$.
  - Por último, si existiese $b \in P \cap -P$, tendríamos que $-b$ también estaría en P; y por tanto, $0 = b + (-b) \in P$. Pero esto no puede pasar como ya hemos visto antes.

□

Con esto, cualquier cuerpo ordenado es formalmente real. Y recíprocamente, un cuerpo donde -1 no es suma de cuadrados, puede ser dotado de un orden. Este orden vendrá determinado por los elementos maximales encontrados en el conjunto $\mathcal{A}$ de la demostración anterior. Y aplicando el Teorema 1.7, un cuerpo formalmente real tendrá tantos órdenes como maximales tenga $\mathcal{A}$.

Teorema 1.25. *Sea R un cuerpo formalmente real y a un elemento no nulo que no es suma de cuadrados. Existe un orden en R en el cual a es negativo.*

Demostración. Basta aplicar el mismo procedimiento de la demostración anterior al conjunto $\mathcal{A}$ de los subconjuntos de R que sean subgrupo de $(R^*, \cdot)$, cerrado para la suma y que contengan a $P_1 = \{\sum b_i^2 + (-a)\sum c_i^2\}$. □

Corolario 1.26. *Un cuerpo formalmente real R admite un orden único si y sólo si para todo $a \neq 0$, o bien a es suma de cuadrados, o bien, $-a$ es suma de cuadrados.*

Teorema 1.27 ([2], ejercicio 1 p. 634)**.** *Sea R un cuerpo formalmente real. $R(x_1, \ldots, x_n)$ es formalmente real, para cualquier $n \in \mathbb{N}$.*

Demostración. En el Teorema 1.15 definimos un orden en $R(x)$. Usando el Teorema 1.15, tenemos que $R(x)$ es formalmente real. Mediante inducción podemos ver que $R(x_1, \ldots, x_n)$ es formalmente real.

Veamos otra demostración, restringiéndonos a la definición de cuerpo formalmente real. Sea R un cuerpo formalmente real. Si $R(x_1, \ldots, x_n)$ no es formalmente real, entonces existe un número finito de $g_i(x_1, \ldots, x_n) \in R(x_1, \ldots, x_n)$ de modo que $\sum g_i^2(x_1, \ldots, x_n) = -1$. Sustituyendo en $(0, \ldots, 0)$, tendríamos que $\sum g_i^2(0, \ldots, 0) = -1$. Dado que $g_i(0, \ldots, 0) \in R$ para cada i, llegaríamos a que R no es formalmente real; pero esto es absurdo. Por tanto, $R(x_1, \ldots, x_n)$ es formalmente real. □

Capítulo 2

Cuerpos Reales Cerrados

Definición 2.1. *Un cuerpo ordenado (R, P) se dice* ***real cerrado*** *si cumple:*

- *Para cada $x \in P$, existe una raíz cuadrada de x en R.*
- *Todo polinomio de grado impar con coeficientes en R tiene al menos una raíz en R.*

Ejemplo 2.2. *El cuerpo de los números racionales no es real cerrado ya que contiene elementos positivos para los cuales no existe una raíz cuadrada en $\mathbb{Q}$. Ejemplo de ellos son 2, 3, $2/3, \ldots$*

En cambio, como bien sabemos, las dos propiedades de un cuerpo real cerrado se cumplen en $\mathbb{R}$. Para ello, se usa el Axioma de Completitud, el cual dice que todo subconjunto no vacío de números reales que está acotado superiormente, tiene supremo.

Por otra parte, cualquier cuerpo que contenga una raíz cuadrada de -1 no es real cerrado ya que ni siquiera es un cuerpo ordenado.

Teorema 2.3. *El orden de un cuerpo real cerrado es único. Cualquier automorfismo de un cuerpo real cerrado es un isomorfismo ordenado.*

Demostración. Si R es un cuerpo real cerrado, todo elemento positivo es un cuadrado. Por tanto, si $a \neq 0$, o bien a es un cuadrado, o bien, $-a$ es un cuadrado. Mediante el Corolario 1.26, el orden de R es único.

Ahora supongamos que φ es un automorfismo de un cuerpo real cerrado R. Si a es un elemento positivo de R, sabemos que existe un $b \in R$ no nulo tal que $a = b^2$. Por tanto, $\varphi(a) = \varphi(b)^2$, y este elemento también es positivo por ser un elemento cuadrado no nulo. Entonces, φ es un isomorfismo ordenado. $\square$

Teorema 2.4. *Sea F un cuerpo ordenado. Si (E, P) es un cuerpo real cerrado extensión de F y su orden es extensión del orden de F, entonces el subcuerpo de E formado por los elementos algebraicos sobre F también es real cerrado.*

En particular, para cualquier cuerpo real cerrado, su subcuerpo de elementos algebraicos sobre $\mathbb{Q}$ es real cerrado.

Demostración. Supongamos que estamos en las condiciones del Teorema. Sea R el subcuerpo de (E, P) formado por los elementos algebraicos sobre F. Como vimos en el Lema 1.10, R es ordenado con cono positivo $P' = R \cap P$. Podemos comprobar que R es real cerrado:

- Sea $a \in P'$. Como E es real cerrado, existe $b \in E$ tal que $a = b^2$. Este b es algebraico sobre R ya que se anula en $x^2 - a \in R[x]$; entonces, $R(b)/R$ es algebraica. Como R es una extensión algebraica de F, b también es algebraico sobre F. Por tanto, b pertenece a R.
- Sea $f(x) \in R[x]$ un polinomio de grado impar. Por ser E real cerrado, existe $c \in E$ tal que $f(c) = 0$. Por el mismo motivo que antes, $c \in R$ y entonces $f(x)$ tiene una raíz en R.

□

Como hemos ido deduciendo, hay muchas similitudes entre el cuerpo $\mathbb{R}$ y los reales cerrados. Ahora veremos una extensión del Teorema Fundamental del Álgebra, pero aplicado a los reales cerrados:

Teorema 2.5. *Si R es un cuerpo real cerrado, entonces $C = R(\sqrt{-1})$ es algebraicamente cerrado.*

Son conocidas muchas demostraciones de este teorema para el cuerpo de los números reales. Muchas de estas demostraciones hacen uso de resultados de Análisis; y estos a su vez, dependen del ya comentado Axioma de Completitud. La demostración que vamos a ver consistirá básicamente en ver que no existe ninguna extensión propia de $C = R(\sqrt{-1})$. Para ello, tan sólo necesitamos suponer las dos condiciones de la Definición 2.1; esto hace que esta demostración sea una de las más débiles.

Para mayor comodidad, denotaremos[1] por i al elemento $\sqrt{-1}$. Si $r = a + bi$ es un elemento de C, el elemento $a - bi$ diremos que es su conjugado y se denotará por $\overline{r}$. Se cumplen dos propiedades que serán útiles más adelante:

- $r\overline{r} = (a + bi)(a - bi) = a^2 + b^2 \in R$.
- $\overline{r^2} = \overline{a^2 - b^2 + 2abi} = a^2 - b^2 - 2abi = (a - bi)^2 = \overline{r}^2$.

Antes de dar la demostración del Teorema 2.5, primero veamos lo siguiente:

Lema 2.6. *Si R es un cuerpo real cerrado, no existe ninguna extensión de grado 2 sobre $C = R(i)$.*

Demostración. Esta demostración se resume en ver que todo polinomio mónico de grado 2 con coeficientes en C tiene sus raíces en C. Sabemos que para cualquier polinomio $x^2 + cx + d$, sus raíces son $(-c \pm \sqrt{c^2 - 4d})/2$; así, basta

[1] Notación que se seguirá utilizando más adelante.

probar que todo elemento de C tiene raíz cuadrada en C. En lo sucesivo de esta demostración, dado un elemento positivo de R, a, denotaremos por $\sqrt{a}$ a la raíz cuadrada positiva de a.

Dado que R es un cuerpo real cerrado, existe una raíz cuadrada en R para todo elemento positivo de R. Si a es un elemento negativo de R, sabemos que existe b tal que $b^2 = -a$; una raíz cuadrada de a será bi.

Tomemos ahora $a + bi \in C$, con $b \neq 0$. Buscamos x, $y \in R$ de modo que $(x + yi)^2 = a + bi$; esto es equivalente a que estos dos elementos cumplan:

$$x^2 - y^2 = a, \qquad 2xy = b.$$

En la segunda ecuación podemos ver que x e y son no nulos ya que $b \neq 0$. Despejando de la misma, tenemos que $y = \frac{b}{2x}$. Sustituyendo en la primera ecuación, se cumple: $4y^4 + 4ay^2 - b^2 = 0$. Como se ha dicho antes, una solución a esta ecuación es $y^2 = (-a + \sqrt{a^2 + b^2})/2$. Dado que $b \neq 0$ y $a^2 + b^2 > 0$, podemos definir correctamente el elemento y^2. Ahora queda ver si existe una raíz cuadrada de y^2. Esta raíz existirá si $-a + \sqrt{a^2 + b^2}$ es positivo en R. Si tuviésemos lo contrario, $-a + \sqrt{a^2 + b^2} \leq 0$; como $\sqrt{a^2 + b^2}$ es positivo, tendríamos que $a^2 + b^2 \leq a^2$; pero como $b \neq 0$, esto no es posible. Por tanto, podemos encontrar x e $y \in R$ cumpliendo las ecuaciones expuestas antes.

Concluimos con que todo elemento de C tiene una raíz cuadrada en C y no existe ningún polinomio mónico irreducible de grado 2 con coeficientes en C. □

Ahora ya podemos dar la demostración del Teorema 2.5. Hemos de saber que utilizaremos el Primer Teorema de Sylow. Su demostración está explicada en el Apéndice A.

Teorema 2.7 (Primer Teorema de Sylow)**.** *Sea G un grupo finito de orden $p^n m$, con p primo, $n \geq 1$ y $(p, m) = 1$. Existe un subgrupo de G de orden p^i, para cada $1 \leq i \leq n$. Además, todo subgrupo de G de orden p^i $(i < n)$ es normal en algún otro subgrupo de orden p^{i+1}.*

Demostración del Teorema 2.5. Supongamos que tenemos un polinomio $f(x)$ con coeficientes en C mónico e irreducible de grado $n > 1$. Sea F el cuerpo de escisión de $f(x)$ sobre C. Tenemos que $[F : C] \leq n!$, y por tanto F/C es finita y algebraica. Con ello, F/R también es finita y algebraica. Además, como la característica es 0, F/R es separable. Ahora consideremos la clausura normal E de F/R. Tenemos que E/R es finita y de Galois; además, E contiene a C por cómo lo hemos construido.

Sea G el grupo de Galois de E/R. Tenemos que $|G| = 2^e m$, con m impar. Por el Teorema 2.7, G contiene un subgrupo H de orden 2^e. Sea K el cuerpo intermedio de E/R fijado por H. Tenemos que la extensión K/R es finita de dimensión m, y además es separable por ser la característica 0. Por el Teorema del Elemento Primitivo, existe $u \in K$ tal que $K = R(u)$. El polinomio mínimo

de u sobre R tiene grado m; pero como R es real cerrado, tan sólo es posible que m sea 1.

Entonces, $K = R$ y $[E : R] = 2^e = |G|$. Dado que $[C : R] = 2$, e es como mínimo 1; supongamos que $e > 1$. Sea G_1 el subgrupo de G que fija a C. De nuevo, por el Teorema 2.7, G_1 contiene un subgrupo D de orden 2^{e-2}. Sea J es el cuerpo intermedio de E/R fijado por D; este tiene dimensión 2^2 sobre R. Con ello tendríamos que $[J : C] = 2$, pero como vimos en el Lema 2.6 esto no puede ocurrir. Por tanto, e sólo puede valer 1 y la supuesta extensión E de C es el propio C. En conclusión, el polinomio $f(x)$ con el que comenzamos no puede ser irreducible de grado mayor que 1, por lo que C es algebraicamente cerrado. □

Así, $C = R(i)$ es una clausura algebraica de R y cualquier extensión algebraica de R debe estar contenida en C/R. Como $[C : R] = 2$, la única extensión algebraica propia de R es C. Además, los polinomios irreducibles de $R[x]$ tienen grado menor o igual que 2. Por la fórmula de resolución de ecuaciones cuadráticas, un polinomio $x^2 + ax + b \in R[x]$ tendrá sus raíces en R si y sólo si $a^2 \geq 4b$.

2.1. Caracterizaciones de los Cuerpos Reales Cerrados

A continuación, vamos a ver tres caracterizaciones de un cuerpo real cerrado. Artin y Schreier dieron otra caracterización, pero debido a que su demostración es muy larga, se dejará para el último capítulo.

Todas las caracterizaciones las conocemos para $\mathbb{R}$, pero veremos que se pueden aplicar para cualquier real cerrado. La primera caracterización tiene que ver con el Teorema del Valor Intermedio:

Definición 2.8. *Se dice que un cuerpo ordenado $(R, \leq)$ tiene la* ***propiedad del valor intermedio****, si para cualquier polinomio $f(x) \in R[x]$ en el que existen a, $b \in R$ con $f(a)f(b) < 0$, se cumple que $f(c) = 0$ para algún $c \in R$ entre a y b.*

Teorema 2.9. *Un cuerpo ordenado es real cerrado si y sólo si tiene la propiedad del valor intermedio.*

Para la demostración de este teorema es necesario ver el siguiente Lema:

Lema 2.10. *Sea $f(x) = a_n x^n + \ldots + a_1 x + a_0$, $a_n \neq 0$, un polinomio con coeficientes en un cuerpo ordenado R. Si t es un elemento de R cumpliendo*

$$|t| > 2 \sum_{i=0}^{n} \left| \frac{a_i}{a_n} \right|,$$

entonces $f(t)$ y $a_n t^n$ tienen el mismo signo.

Demostración. Supongamos las condiciones del Lema. Dado que el sumatorio del enunciado es mayor que 1, podemos concluir que $|t| > 2$ y que $t \neq 0$. Para ver que $f(t)$ y $a_n t^n$ tienen el mismo signo, los comparamos dividiéndolos:

$$\frac{f(t)}{a_n t^n} = \frac{a_n t^n + \ldots + a_1 t + a_0}{a_n t^n} = 1 + \sum_{i=0}^{n-1} \frac{a_i}{a_n} t^{i-n}$$

Ahora tan sólo quedar ver que este valor es mayor que 0. Para ello, aprovechando las hipótesis y que estamos en un cuerpo ordenado, vamos a utilizar algunas de las propiedades del valor absoluto: es siempre no negativo, $-|a| \leq a$, $|a+b| \leq |a| + |b|$, $|ab| = |a||b|, \ldots$

Dado que $\displaystyle\sum_{i=0}^{n-1} \frac{a_i}{a_n} t^{i-n} \geq -\left|\sum_{i=0}^{n-1} \frac{a_i}{a_n} t^{i-n}\right| \geq -\sum_{i=0}^{n-1} \left|\frac{a_i}{a_n}\right| |t|^{i-n}$, se cumple que:

$$1 + \sum_{i=0}^{n-1} \frac{a_i}{a_n} t^{i-n} \geq 1 - \sum_{i=0}^{n-1} \left|\frac{a_i}{a_n}\right| |t|^{i-n} \geq 1 - \sum_{i=0}^{n-1} \left|\frac{a_i}{a_n}\right| \sum_{j=0}^{n-1} |t|^{j-n}$$
$$\geq 1 - \sum_{i=0}^{n} \left|\frac{a_i}{a_n}\right| (|t|^{-1} + \ldots + |t|^{-n})$$

Como por hipótesis tenemos que $\frac{|t|}{2} > \displaystyle\sum_{i=0}^{n} \left|\frac{a_i}{a_n}\right|$, se cumple que:

$$\frac{f(t)}{a_n t^n} \geq 1 - \frac{|t|}{2}(|t|^{-1} + \ldots + |t|^{-n}) = 1 - \frac{1}{2}(1 + \ldots + |t|^{-n+1}) = 1 + \frac{1}{2}\left(\frac{1 - |t|^{-n}}{1 - |t|^{-1}}\right).$$

Simplificando el elemento que está entre paréntesis, vemos que es igual a $\frac{t^n - 1}{t^n - t^{n-1}}$. Este elemento es positivo ya que $|t|$ es mayor que 2. Por tanto, podemos concluir que $\frac{f(t)}{a_n t^n} > 0$ y con ello, $f(t)$ y $a_n t^n$ tienen el mismo signo. □

Demostración del Teorema 2.9. Sea R un cuerpo real cerrado y $f(x)$ un polinomio con coeficientes en R. Supongamos que f es mónico y que existen a y $b \in R$ de modo que $f(a)f(b) < 0$. Vamos a ver que existe un elemento de R entre a y b que anula a f.

Dado que $C = R(i)$ es algebraicamente cerrado, este contiene a todas las raíces de f. Sabemos además que su factorización en irreducibles en R tan sólo tiene elementos de grado 1 o 2:

$$f(x) = (x - r_1) \ldots (x - r_m) g_1(x) \ldots g_s(x) = \prod_{i=0}^{m} (x - r_i) \prod_{j=0}^{s} g_j(x)$$

Como los g_i son irreducibles en $R[x]$, sus raíces están en $C \setminus R$. Si $c + di$, $d \neq 0$, es raíz de g_{i_0}, entonces $c - di$ también es raíz de g_{i_0} debido a que

$g_{i_0}(c+di)$ y $g_{i_0}(c-di)$ también son conjugados. Por tanto, los g_i son de la forma $(x-c)^2+d^2=(x-c-di)(x-c+di)$. Como $d\neq 0$, tenemos que $g_i(t)>0$ para todo $t\in R$.

Ahora veamos que alguno de los $r_i\in R$ debe de estar entre a y b. Si tuviésemos que $a,\ b<r_i$, para todo $i=1,\ldots,m$, tendríamos que $f(a)f(b)$ sería mayor que 0 ya que

$$f(a)f(b)=\prod_{i=0}^{m}(a-r_i)(b-r_i)\prod_{j=0}^{s}g_j(a)g_j(b),$$

pero esto no puede ocurrir porque hemos supuesto que $f(a)f(b)<0$. Sucede lo mismo si suponemos que $r_i<a,\ b$ para todo $i=1,\ldots,m$. Por tanto, uno de los r_i tiene que estar entre a y b.

Por otra parte, supongamos que $(R,\leq)$ es un cuerpo ordenado donde se cumple la propiedad del valor intermedio. Gracias al Lema 2.10, podemos ver que se cumplen las condiciones de la Definición 2.1 de real cerrado:

- Sea $0<a$. Consideremos el polinomio $p(x)=x^2-a\in R[x]$. Por el Lema 2.10, existe un $t\in R$, lo suficientemente grande, tal que $p(t)$ tiene el mismo signo que t^2; es decir, $p(t)>0$. Dado que $p(0)=-a<0$, por la propiedad del valor intermedio existe $c\in R$ entre 0 y t de modo que $c^2-a=0$. Hemos encontrado una raíz cuadrada de a en R.

- Sea $f(x)\in R[x]$ un polinomio de grado impar. Usando el Lema 2.10 de nuevo, vemos que para un t_1 lo suficientemente grande, $f(t_1)$ es positivo; y para un t_2 lo suficientemente pequeño, $f(t_2)$ es negativo. Por tanto, por la propiedad del valor intermedio, existe $t\in R$ entre t_1 y t_2 de modo que $f(t)=0$.

Entonces, R es un cuerpo real cerrado, como queríamos demostrar. □

A partir de que en todo cuerpo real cerrado se cumple la propiedad del valor intermedio, se puede demostrar que se cumplen otras propiedades conocidas para $\mathbb{R}$; tales como: Teorema de Rolle, Teorema de Weierstrass, Teorema del valor medio, ... (véase [4], p. 35).

La siguiente caracterización de un cuerpo real cerrado tiene que ver con su relación con los cuerpos formalmente reales. En el Teorema 1.24, hemos demostrado que las nociones de cuerpo formalmente real y cuerpo ordenable son equivalentes; por ello, todo cuerpo real cerrado es formalmente real. El recíproco no es trivial, ya que, como hemos dicho, no todo cuerpo ordenado es real cerrado. Hay que agregar otra condición, que será justificada con el siguiente Lema:

Lema 2.11. *Sea F un cuerpo formalmente real y r un elemento algebraico sobre F. Si*

- *r es raíz cuadrada de algún elemento positivo de F (en algún orden de F), o si*
- *r tiene polinomio mínimo sobre F de grado impar,*

entonces $F(r)$ es formalmente real.

Demostración. Veamos el primer caso. Tenemos que $r^2 = a$ para algún $a > 0$ de F. Por reducción al absurdo, supongamos que $F(r)$ no es formalmente real. Como F sí es formalmente real, entonces $r \notin F$ y $[F(r) : F] = 2$. Al tener que $F(r)$ no es formalmente real, existe un número finito de a_i, $b_i \in F$ cumpliendo $\sum (a_i + b_i r)^2 = -1$. Operando obtenemos: $-1 = \sum (a_i^2 + b_i^2 r^2 + 2a_i b_i r)$; e igualando coeficientes tenemos que $-1 = \sum (a_i^2 + b_i^2 a) = \sum a_i^2 + a \sum b_i^2$. Pero esto no puede ocurrir, ya que a es un elemento positivo y, con ello, la última suma da lugar a un elemento positivo. Por tanto, en este caso $F(r)$ es formalmente real.

Ahora veamos el segundo caso. Sea $f(x)$ el polinomio mínimo de r sobre F. Por hipótesis, el grado de $f(x)$ es impar. Vamos a ver que $F(r)$ es formalmente real mediante inducción en el grado de $f(x)$, m. Si $m = 1$, entonces $r \in F$ y $F(r) = F$ es formalmente real. Ahora supongamos que $m > 1$ y $F(r)$ no es formalmente real. Entonces, existe un número finito de $g_i(x) \in F[x]$ de grado menor que m cumpliendo $\sum g_i(r)^2 = -1$. Volviendo a $F[x]$, como $f(x)$ es el polinomio mínimo de r y $1 + \sum g_i(x)^2$ se anula en r, se cumple que

$$1 + \sum g_i(x)^2 = f(x)g(x), \text{ para algún } g(x) \in F[x]. \tag{2.1}$$

El coeficiente principal de cada $g_i(x)^2$ es un cuadrado; por ello, $deg(g_i(x)^2 + g_j(x)^2) = max\{deg(g_i(x)^2), deg(g_j(x)^2)\}$ ya que la suma de dos cuadrados no puede ser nula (F es formalmente real y ordenado). Con esto, $deg(1+\sum g_i(x)^2)$ es par y menor que $2m$. Y ahora, como $deg(1+\sum g_i(x)^2) = deg(f(x)g(x))$ y el grado de f, m, es impar, es necesario que el grado de $g(x)$ también sea impar y menor que m.

Tomemos $h(x)$ un factor mónico e irreducible de $g(x)$ de grado impar. Sea $F(u)$ un cuerpo raíz de $h(x)$ sobre F. Dado que $deg(h(x)) < m$, $F(u)$ es formalmente real por la hipótesis de inducción. Volviendo a la ecuación (2.1) tenemos que $1 + \sum g_i(u)^2 = f(u)g(u) = 0$ y entonces $\sum g_i(u)^2 = -1$, lo que se contradice con que $F(u)$ sea formalmente real. Por tanto, en este caso, $F(r)$ también es formalmente real. □

Entonces, la caracterización de los cuerpos reales cerrados que los relaciona con los cuerpos formalmente reales es la siguiente:

Teorema 2.12. *Un cuerpo R es real cerrado si y sólo si es formalmente real y no tiene ninguna extensión algebraica propia que sea formalmente real.*

Demostración. Supongamos que R es un cuerpo real cerrado. Como R es ordenado, por el Teorema 1.24, R es formalmente real. Como vimos en el Teorema 2.5, $C = R(i)$ es algebraicamente cerrado y la única extensión propia de R es C, que no es formalmente real ya que $i \in C$.

Supongamos ahora que R es un cuerpo formalmente real y que ninguna extensión algebraica propia de R es formalmente real. Veamos si se cumplan las condiciones de un cuerpo real cerrado:

- Sea a un elemento positivo de R, en algún orden de R, y b una raíz cuadrada de a. Por el Lema 2.11, $R(b)$ es formalmente real. Dado que R no tiene extensiones propias formalmente reales, se tiene que cumplir que $R(b) = R$ y por tanto $b \in R$. Con esto, podemos deducir que R tiene un único orden.

- Sea $f(x) \in R[x]$ un polinomio de grado impar. Tomemos $g(x)$ un factor irreducible de $f(x)$ de grado impar. Sea $R(c)$ un cuerpo raíz de $g(x)$ sobre R. Por el Lema 2.11, $R(c)$ es formalmente real; por tanto, $R(c) = R$ y $c \in R$. Como $g(c) = 0$ y $g(x)$ es un factor de $f(x)$, tenemos que $f(c) = 0$.

Por tanto, R es real cerrado. □

La última caracterización que vamos a ver en este capítulo, es lo que se puede considerar: el recíproco del Teorema 2.5. Pero para que se cumpla, es necesario agregar una condición obviamente necesaria:

Teorema 2.13. *Un cuerpo R es real cerrado si y sólo si $\sqrt{-1} \notin R$ y $R(\sqrt{-1})$ es algebraicamente cerrado.*

Demostración. Sabemos que un cuerpo real cerrado no puede contener una raíz cuadrada de -1 ya que sería una contradicción con que sea ordenado. En el Teorema 2.5 vimos que la extensión de un cuerpo real cerrado generada por $i = \sqrt{-1}$ es algebraicamente cerrado. Así que ya teníamos la primera implicación probada. Para el recíproco usaremos el Teorema 2.12 anterior.

Supongamos que R es un cuerpo que no contiene a ninguna raíz de -1 y que $C = R(i)$ es algebraicamente cerrado. Para ver que R es formalmente real, primero hemos de ver que la suma finita de cuadrados en R es otro cuadrado de R. Sean $a, b \in R$; como C es algebraicamente cerrado, existe $u \in C$ cumpliendo $u^2 = a + bi$. Ahora:

$$a^2 + b^2 = (a + bi)(a - bi) = u^2\overline{u^2} = (u\overline{u})^2.$$

Dado que para cualquier $r \in C$, $r\overline{r} \in R$, tenemos que $a^2 + b^2 = (u\overline{u})^2$ es otro cuadrado de R. Mediante inducción, tenemos que cualquier suma finita de elementos cuadrados de R es un cuadrado de R. Dado que $i \notin R$, -1 no es un cuadrado en R; por tanto, -1 no es suma de cuadrados de R. Ya tenemos que R es formalmente real.

Por último, dado que i no pertenece a R, tenemos que $R \subsetneq R(i)$ y $[R(i) : R] = 2$. Como además, $R(i)$ es algebraicamente cerrado, la única extensión algebraica propia de R es $R(i)$. $R(i)$ no es formalmente real ya que contiene a i; por tanto, por el Teorema 2.12, R es real cerrado. □

No debemos perder de vista a este último teorema, ya que será utilizado en la caracterización de cuerpos reales cerrados dada por Artin-Schreier, que veremos en el último capítulo. Antes de eso, en el siguiente capítulo veremos otro de los trabajos de Artin y Schreier. Se trata de la existencia y unicidad, salvo isomorfismos ordenados, de una clausura real para cualquier cuerpo ordenado. Pero para facilitar su demostración, primero tenemos que explicar el Teorema de Sturm.

2.2. Teorema de Sturm

Dado un cuerpo real cerrado R y un polinomio con coeficientes en él, el teorema de Sturm nos permite calcular el número de raíces distintas que tiene en un intervalo contenido en el cuerpo R. Antes de introducir el teorema, hemos de dar la noción de sucesión de Sturm:

Definición 2.14. *Sea $f(x)$ un polinomio de grado positivo con coeficientes en un cuerpo real cerrado R. Diremos que una sucesión de polinomios de $R[x]$*

$$f_0(x) = f(x), f_1(x), \ldots, f_s(x)$$

*es una **sucesión de Sturm** de $f(x)$ en el intervalo $[a, b]$, si se cumple lo siguiente:*

1. *$f_s(x)$ no tiene raíces en $[a, b]$.*
2. *$f_0(a)f_0(b) \neq 0$.*
3. *Si $c \in [a, b]$ es una raíz de $f_j(x)$, $0 < j < s$, entonces $f_{j-1}(c)f_{j+1}(c) < 0$.*
4. *Si $f(c) = 0$ para algún $c \in [a, b]$, existen intervalos (c_1, c) y (c, c_2) tales que $f_0(t)f_1(t) < 0$ para todo $t \in (c_1, c)$ y $f_0(t)f_1(t) > 0$ para todo $t \in (c, c_2)$.*

Dada una sucesión de Sturm $f_0(x), \ldots, f_s(x)$ de un polinomio $f(x)$ en un intervalo $[a, b]$, para poder calcular el número de raíces distintas que tiene $f(x)$ en el intervalo, hemos de calcular el número de cambios de signo en las siguientes sucesiones:

$$f_0(a), f_1(a), \ldots, f_s(a)$$
$$f_0(b), f_1(b), \ldots, f_s(b).$$

Donde los cambios de signo es lo que se espera (la sucesión -2, 3, 0, 1, 2, -1 tiene 2 cambios de signo). Veámoslo en el siguiente teorema:

Teorema 2.15. *Sea $f(x)$ un polinomio de grado positivo con coeficientes en un cuerpo real cerrado R. Si $f_0(x) = f(x), \ldots, f_s(x)$ es una sucesión de Sturm de $f(x)$ en un intervalo $[a, b]$ de R, el número de raíces distintas de $f(x)$ contenidas en $[a, b]$ es $V_a - V_b$, donde V_c es el número de cambios de signo de la sucesión $f_0(c), \ldots, f_s(c)$.*

Demostración. Supongamos que estamos en las condiciones del teorema. Hemos de ver que el valor $V_a - V_b$ coincide con el número de raíces que tiene $f(x)$ en el intervalo $[a, b]$. Podemos descomponer este intervalo por las raíces de todos los polinomios $f_j(x)$ de la sucesión de Sturm (las raíces de $f(x)$ están incluidas). Así, obtenemos una sucesión $a = a_0 < a_1 < \ldots < a_m = b$ de modo que ninguno de los $f_j(x)$ tiene una raíz en los subintervalos (a_{i-1}, a_i), $1 \leq i \leq m$. Ahora, tomando un c_i en cada uno de estos subintervalos, podemos expresar $V_a - V_b$ de la siguiente forma:

$$V_a - V_b = V_{a_0} - V_{a_m} = (V_{a_0} - V_{c_1}) + \sum_{i=1}^{m-1} (V_{c_i} - V_{c_{i+1}}) + (V_{c_m} - V_{a_m}). \quad (2.2)$$

Hemos de ver que el valor de la derecha coincide con el número de raíces que tiene $f(x)$ en el intervalo $[a, b]$. Podemos comprobar que el primer paréntesis vale 0. Dado que R es un cuerpo real cerrado, por el Teorema 2.9, se cumple la propiedad del valor intermedio. Así, como ninguno de los $f_j(x)$ se anula en el intervalo (a_0, c_1), $f_j(a_0)f_j(c_1) \geq 0$ para todo j. Recordemos que ninguno de los $f_j(x)$ se anula en los c_i; por tanto, si ninguno de los $f_j(x)$ se anula en a_0, se tiene que $f_j(a_0)f_j(c_1) > 0$ para todo j. De esta forma, todas las parejas $f_j(a_0)$ - $f_j(c_1)$ tienen el mismo signo y $V_{a_0} = V_{c_1}$.

Ahora supongamos que existe un k de modo que $f_k(a_0) = 0$. Por las dos primeras propiedades de una sucesión de Sturm (Definición 2.14), este k es distinto de 0 y s. Entonces, por la tercera propiedad se tiene que $f_{k-1}(a_0)f_{k+1}(a_0) < 0$. Como $f_{k-1}(x)$ y $f_{k+1}(x)$ no se anulan en (a_0, c_1), aplicando de nuevo el Teorema del Valor Intermedio, $f_{k-1}(a_0)f_{k-1}(c_1) > 0$ y $f_{k+1}(a_0)f_{k+1}(c_1) > 0$ (no nulos porque $f_{k-1}(a_0)f_{k+1}(a_0) < 0$). Por tanto, es necesario que también se cumpla que $f_{k-1}(c_1)f_{k+1}(c_1) < 0$. Así, las subsucesiones $f_{k-1}(a_0)$, $f_k(a_0)$, $f_{k+1}(a_0)$ y $f_{k-1}(c_1)$, $f_k(c_1)$, $f_{k+1}(c_1)$ aportan un cambio de signo a V_{a_0} y V_{c_1} respectivamente. Realizando lo mismo para cada k tal que $f_k(a_0) = 0$, también se llega a que $V_{a_0} = V_{c_1}$.

Con un razonamiento similar, se puede ver que $V_{c_m} = V_{a_m}$. Por ello, el último paréntesis de la ecuación 2.2 también es nulo.

Por último, veamos cuánto vale el sumatorio. Para cada $i = 1, \ldots, m-1$, si $f(a_i) \neq 0$, el mismo razonamiento de antes nos hace llegar a que $V_{c_i} = V_{c_{i+1}}$ (tal y como nos interesa). Ahora veamos que si $f(a_i) = 0$, entonces $V_{c_i} - V_{c_{i+1}} = 1$. Por la cuarta propiedad de una sucesión de Sturm, existen intervalos $[z_1, a_i)$ y $(a_i, z_2]$ (nos interesan intervalos cerrados en este caso) tales que $f_0(t)f_1(t) < 0$ para todo $t \in [z_1, a_i)$ y $f_0(t)f_1(t) > 0$ para todo $t \in (a_i, z_2]$. Podemos suponer que $a_{i-1} < z_1$ y $z_2 < a_{i+1}$. Como ninguno de los $f_j(x)$ se anula en el intervalo

que hay entre (a_{i-1}, a_i), entonces $V_t = V_{c_i}$ para todo $t \in (a_{i-1}, a_i)$; en particular, $V_{z_1} = V_{c_i}$. De la misma manera, $V_{c_{i+1}} = V_{z_2}$.

Por tanto, por la cuarta propiedad de una sucesión de Sturm, $f_0(c_i)f_1(c_i) < 0$ y $f_0(c_{i+1})f_1(c_{i+1}) > 0$. Así, la subsucesión $f_0(c_i)$, $f_1(c_i)$ tiene un cambio de signo, mientras que la subsucesión $f_0(c_{i+1})$, $f_1(c_{i+1})$ ninguno. Con el mismo razonamiento que se ha hecho al principio, se puede ver que las demás f_j de las sucesiones $(f_j(c_i))$ y $(f_j(c_{i+1}))$ tienen el mismo número de cambios de signo. Por tanto, $V_{c_i} = V_{c_{i+1}} + 1$. Y concluimos que el valor $V_a - V_b$ coincide con el número de raíces que tiene $f(x)$ en el intervalo $[a, b]$. □

Pero, para aplicar el Teorema anterior a un polinomio, es necesario encontrar una sucesión de Sturm del polinomio. A continuación, vamos a dar una sucesión de polinomios que en algunos casos será una sucesión de Sturm, pero en otros no (dependiendo de si el polinomio tiene raíces múltiples o no).

Definición 2.16. *Sea $f(x)$ un polinomio de grado positivo con coeficientes en un cuerpo ordenado. Fijando $f_0(x) = f(x)$ y $f_1(x) = f'(x)$ (derivada formal de $f(x)$), los siguientes $f_i(x)$ se obtienen mediante el algoritmo de Euclides, pero cambiando de signo a los restos:*

$$f_{i+1}(x) = q_i(x)f_i(x) - f_{i-1}(x), \qquad deg(f_{i+1}(x)) < deg(f_i(x)). \tag{2.3}$$

Como bien sabemos, existe un $s+1$ tal que $f_{s+1}(x) = 0$ y $f_s(x)$ es el máximo común divisor de $f(x)$ y $f'(x)$. Esta sucesión de s polinomios la denominaremos **sucesión estándar de** $f(x)$.

Los dos siguientes resultados son los que nos permiten calcular el números de raíces distintas de cualquier polinomio. Sus demostraciones están remitidas a la bibliografía ([1]).

Teorema 2.17. *Sea $f(x)$ un polinomio de grado positivo con coeficientes en un cuerpo real cerrado. La sucesión estándar de $f(x)$ es una sucesión de Sturm de $f(x)$ para cualquier intervalo $[a, b]$ que cumpla:*

- *$[a, b]$ no contiene ninguna raíz múltiple de $f(x)$.*
- *$f(a)f(b) \neq 0$.*

Teorema 2.18 (Teorema de Sturm)**.** *Sea $f(x)$ un polinomio de grado positivo con coeficientes en un cuerpo real cerrado R y $(f_i(x))_i$ su sucesión estándar. Si $[a, b]$ es un intervalo de R tal que $f(a)f(b) \neq 0$, el número de raíces distintas de $f(x)$ contenidas en el intervalo es $V_a - V_b$.*

Demostración. Consideremos la sucesión $g_i(x) = f_i(x)f_s(x)^{-1}$, $i = 0, \ldots, s$. Como $f_s(x)$ es el máximo común divisor de $f(x)$ y $f'(x)$, $f(x)$ y $g_0(x)$ tienen las mismas raíces, pero en el caso de g_0 todas las raíces son simples. Mediante el Teorema 2.17 anterior, la sucesión $(g_i(x))_i$ es una sucesión de Sturm de $g_0(x)$ para el intervalo $[a, b]$. Usando el Teorema 2.15 y el hecho de que $f_s(x)$ no se anula en el intervalo $[a, b]$, el número de raíces distintas de $f(x)$ en el intervalo es $V_a - V_b$. □

Capítulo 3

Clausura Real

Teorema 3.1. *Para cualquier cuerpo ordenado F, existe una extensión R de F cumpliendo:*

- *R es real cerrado.*
- *R/F es algebraica.*
- *El orden (único) de R es extensión del orden de F.*

Demostración. Sea F un cuerpo ordenado y $\bar{F}$ una clausura algebraica de F. Como queremos que el orden de R sea extensión del orden de F, podemos tomar la subextensión de $\bar{F}/F$ generada por las raíces cuadradas de todos los elementos positivos de F. Así, los elementos positivos de F serán cuadrados en R. Llamemos E a esta subextensión y veamos que es formalmente real. Si no fuese así, existiría un número finito de $a_i \in E$ de modo que $\sum a_i^2 = -1$. Cada a_i es resultado de una combinación sobre F de raíces cuadradas de elementos positivos de F; por ello, cada a_i pertenece a la extensión de F generada por estas raíces cuadradas. Entonces, tenemos que todos los a_i están contenidos en una extensión, L, de F generada por un número finito de raíces cuadradas de elementos positivos de F. Pero esto no puede ocurrir, ya que haciendo inducción con el Lema 2.11, tenemos que L es formalmente real y no podría cumplirse que $\sum a_i^2 = -1$.

Ahora, denotemos por $\mathcal{S}$ al conjunto de subconjuntos de $\bar{F}$ que sean extensiones algebraicas de E y además sean formalmente reales. Este conjunto obviamente no es vacío ya que al menos E pertenece a él. Consideremos, en $\mathcal{S}$, el contenido $\subseteq$ como relación de orden parcial y veamos que podemos encontrar un maximal aplicando el Lema de Zorn (Lema 1.22, pág. 17).

Sea $\{E_i\}_{i\in I}$ una cadena en $\mathcal{S}$. Podemos probar que $K = \bigcup_{i\in I} E_i$ (cota superior de la cadena) pertenece a $\mathcal{S}$:

- Dado que todo elemento de $\mathcal{S}$ es cuerpo intermedio de $\bar{F}/F$, se cumple que $K \subseteq \bar{F}$. Además, como E está contenido en todo elemento de $\mathcal{S}$, K

es no vacío ya que al menos contiene a E. Para probar que K es cuerpo, basta con probar que si a, $b \in K$, entonces $a - b \in K$; y si c, $d \in K^*$, entonces $cd^{-1} \in K^*$. Ambas cosas se pueden probar de forma similar a como se hizo en la demostración del Teorema 1.24 (pág. 18), usando la definición de cadena.

- K es formalmente real: si no fuese así, existiría un número finito de $a_i \in K$ de modo que $\sum a_i^2 = -1$. Tomando la misma idea que en la demostración del Teorema 1.24, existiría un E_i en la cadena conteniendo a todos los a_i. Pero esto no puede ocurrir porque todos los elementos de $\mathcal{S}$ son formalmente reales.

- K/E es algebraica: si $a \in K$, $a \in E_i$ para algún $i \in I$. Dado que todos los elementos de $\mathcal{S}$ son extensiones algebraicas de E, a es algebraico sobre E.

Dado que estamos en las condiciones para aplicar el Lema de Zorn, podemos encontrar un maximal R en $\mathcal{S}$. Entonces, este R es un cuerpo formalmente real y extensión algebraica de E. Además, R es cuerpo intermedio de $\bar{F}/F$.

Podemos comprobar que R es real cerrado. Si no fuese así, por el Teorema 2.12, R tendría al menos una extensión algebraica propia formalmente real, R'. Como $\bar{F}$ no puede ser formalmente real por ser algebraicamente cerrado (contiene a una raíz cuadrada de -1), R' es un subcuerpo propio de $\bar{F}/F$. Entonces, R' es otro elemento de $\mathcal{S}$ que contiene estrictamente a R. Pero esto es absurdo ya que R es un elemento maximal. Por tanto, R es real cerrado.

Por último, el orden de R (único por el Teorema 2.3) es extensión del orden de F por como hemos construido R. □

Definición 3.2. *Dado un cuerpo ordenado F, llamaremos* ***clausura real*** *de F a un cuerpo extensión de F con las propiedades del Teorema anterior.*

Ejemplo 3.3. *El cuerpo $\mathbb{R}$ no puede ser una clausura real de $\mathbb{Q}$, debido a que $\mathbb{R}/\mathbb{Q}$ no es una extensión algebraica. En el Teorema 2.4 vimos que la subextensión formada por los elementos algebraicos sobre $\mathbb{Q}$, es un cuerpo real cerrado. Dado que el orden de cualquier cuerpo ordenado es extensión del orden (único) de $\mathbb{Q}$, el cuerpo de los números reales algebraicos sobre $\mathbb{Q}$ es una clausura real de $\mathbb{Q}$.*

Teorema 3.4 ([2], ejercicio 1 p. 637)**.** *Sea F un cuerpo ordenado. Si E es un cuerpo real cerrado extensión de F, y su orden es extensión del orden de F, entonces E contiene una clausura real de F.*

Demostración. Supongamos que estamos en las condiciones del Teorema. Por el Teorema 2.4, el subcuerpo de E formado por los elementos algebraicos sobre F, R, es un real cerrado. También se cumple que R es una extensión algebraica de F.

Por último, como el orden de R es el inducido por E y el orden de E es extensión del orden de F, tenemos que el orden de R es extensión del orden de F. Por tanto, R es una clausura real de F. □

En el Teorema 3.7 vamos a probar la unicidad, salvo isomorfismos ordenados, de la clausura real. Pero antes, hemos de demostrar los siguientes lemas:

Lema 3.5. *Sean R_1 y R_2 dos cuerpos reales cerrados, F_i un subcuerpo de R_i, $i = 1, 2$. Supongamos que φ es un isomorfismo ordenado de F_1 en F_2, donde el orden de F_i es el inducido por R_i. Si $f(x)$ es un polinomio mónico de $F_1[x]$ y $\bar{f}(x) \in F_2[x]$ es el polinomio obtenido al aplicar φ a los coeficientes de $f(x)$[1], entonces $f(x)$ tiene el mismo número de raíces distintas en R_1 que $\bar{f}(x)$ en R_2.*

Demostración. Supongamos que estamos en las condiciones del Lema y que $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ es un polinomio con coeficientes en $F_1 \subseteq R_1$. Por el Teorema 1.9, las raíces contenidas en R_1 de $f(x)$ están en el intervalo $(-M, M)$, donde $M = 1 + |a_{n-1}| + \ldots + |a_0|$. Así, por el teorema de Sturm (p. 31), si $f_0(x) = f(x), f_1(x), \ldots, f_s(x)$ es la sucesión estándar de $f(x)$, el número de raíces distintas que tiene $f(x)$ en R_1 es $V_{-M} - V_M$, donde V_t es el número de cambios de signo en $f_0(t), f_1(t), \ldots, f_s(t)$.

De igual forma, las raíces contenidas en R_2 del polinomio $\bar{f}(x)$, se encuentran en el intervalo $(-M', M')$, donde $M' = 1 + \varphi(a_{n-1})| + \ldots + |\varphi(a_0)|$. Usando una de las propiedades de un isomorfismo ordenado (pág. 15), se puede ver que $\varphi(M) = \varphi(1 + |a_{n-1}| + \ldots + |a_0|) = 1 + |\varphi(a_{n-1})| + \ldots + |\varphi(a_0)| = M'$. Por otra parte, dado que φ es un isomorfismo ordenado, los polinomios $\bar{f}_0(x) = \bar{f}(x), \bar{f}_1(x), \ldots, \bar{f}_s(x)$ forman la sucesión estándar de $\bar{f}(x)$. Así, aplicando de nuevo el teorema de Sturm, el número de raíces distintas en R_2 de $\bar{f}(x)$ es $W_{-\bar{M}} - W_{\bar{M}}$, donde W_t es el número de cambios de signo en $\bar{f}_0(t), \bar{f}_1(t), \ldots, \bar{f}_s(t)$.

Dado que un isomorfismo ordenado se conserva el orden, si $t \in R_1$ y $f_i(t) > 0$ en R_1, entonces $\bar{f}_i(\varphi(t)) > 0$ en R_2. Así, podemos concluir que $V_t = W_{\varphi(t)}$; y con ello, $V_{-M} - V_M = W_{-\bar{M}} - W_{\bar{M}}$. Por tanto, $f(x)$ tiene el mismo número de raíces distintas en R_1 que $\bar{f}(x)$ en R_2, como queríamos probar. □

Lema 3.6. *Sean F_1 y F_2 dos cuerpos ordenados con clausuras reales R_1 y R_2, respectivamente. Supongamos que S es un subconjunto finito de R_1 y φ un isomorfismo ordenado entre F_1 y F_2. Entonces, existe un subcuerpo E_1 de R_1/F_1 conteniendo a S y un monomorfismo $\eta : E_1/F_1 \to R_2/F_2$ que extiende a φ y conserva el orden de los elementos de S.*

Demostración. Supongamos que estamos en las condiciones del Lema y que $S = \{s_1, s_2, \ldots, s_n\} \subseteq R_1$. Dado que R_1 posee un orden, podemos reordenar los elementos de S de modo que nos quede: $s_1 < s_2 < \ldots < s_n$. Entonces,

[1]Esta notación seguirá siendo utilizada más adelante.

$s_{i+1} - s_i$ es un elemento positivo de R_1, para cada $1 \leq i \leq n-1$. Como R_1 es real cerrado, estos elementos tienen raíz cuadrada en R_1. Consideremos entonces el conjunto $T = S \cup \{\sqrt{s_{i+1} - s_i} : 1 \leq i \leq n-1\}$.

Consideremos $E_1 = F_1(T)$. Dado que R_1 es una clausura real de F_1, tenemos que R_1/F_1 es algebraica y S es un subconjunto de elementos algebraicos sobre F_1. Con esto, T es un subconjunto finito de elementos algebraicos sobre F_1. Por tanto, E_1/F_1 es finita. Dado que la característica es 0, por el Teorema del Elemento Primitivo, existe $w \in E_1$ de modo que $E_1 = F_1(w)$.

Sea $f(x)$ el polinomio mínimo de w sobre F_1. Por el Lema 3.5 anterior, tenemos que $\bar{f}(x) = \varphi(f(x))$ tiene al menos una raíz, $\bar{w}$, en R_2. Dado que φ es un isomorfismo, $\bar{f}(x)$ es el polinomio mínimo de $\bar{w}$ sobre F_2. Por tanto, existe un isomorfismo η entre $F_1(w)$ y $F_2(\bar{w})$ que extiende a φ y aplica w en $\bar{w}$.

Ahora, para cada $1 \leq i \leq n-1$, $\eta(s_{i+1}) - \eta(s_i) = \eta(s_{i+1} - s_i)$. Por el modo en que hemos construido E_1, existe $b \in E_1$ no nulo tal que $b^2 = s_{i+1} - s_i$. Por tanto, $\eta(s_{i+1} - s_i) = \eta(b^2) = (\eta(b))^2 > 0$. Entonces, $\eta s_1 < \eta s_2 < \ldots < \eta s_n$ y η conserva el orden de los elementos de S. □

Teorema 3.7. *Sean F_1 y F_2 dos cuerpos ordenados con clausuras reales R_1 y R_2, respectivamente. Todo isomorfismo ordenado entre F_1 y F_2 tiene una única extensión a un isomorfismo ordenado entre R_1 y R_2.*

En particular, si $F_1 = F_2$ y consideramos la identidad en F_1 como isomorfismo ordenado, tenemos que dos clausuras reales de F_1 son isomorfas.

Demostración. Sean F_1 y F_2 dos cuerpos ordenados y φ un isomorfismo ordenado entre ellos. Supongamos que tenemos una clausura real R_i de F_i, $i = 1, 2$. Vamos a definir una aplicación Φ de R_1 a R_2 que extienda a φ y que además sea isomorfismo ordenado.

Sea r un elemento de R_1 y $f_r(x)$ su polinomio mínimo sobre F_1. Consideramos las raíces de $f_r(x)$ en R_1 y las colocamos en orden creciente, según el orden de R_1: $r_1 < r_2 < \ldots < r_k = r < \ldots < r_m$. Por el Lema 3.5, $\bar{f}_r(x) = \varphi(f_r(x))$ también tiene m raíces en R_2; las colocamos en orden creciente, según el orden de R_2: $\bar{r}_1 < \bar{r}_2 < \ldots < \bar{r}_m$. Definimos $\Phi : R_1 \to R_2$ como la aplicación que envía r a la k-sima raíz de $\bar{f}_r(x)$.

Esta aplicación está bien definida, ya que para cada una de las raíces r_i, $f_r(x)$ es su polinomio mínimo sobre F_1. Y dado que φ es un isomorfismo, $\bar{f}_r(x)$ también es mónico e irreducible; por lo que es el polinomio mínimo de cada $\bar{r}_i$ sobre F_2 y todas estas son distintas dos a dos. Está claro que Φ extiende a φ: si $r \in F_1$, su polinomio mínimo sobre F_1 es $f_r(x) = x - r$; por lo que $\bar{f}_r(x) = x - \varphi(r)$ y $\Phi(r) = \varphi(r)$. Ahora veamos que Φ es biyectiva:

- Sean r, $s \in R_1$ y $f_r(x)$, $f_s(x)$ sus respectivos polinomios mínimos sobre F_1. Si $\Phi(r) = \Phi(s) = \bar{r}$, entonces $\bar{r}$ es la k-sima raíz de $\bar{f}_r(x)$ y de $\bar{f}_s(x)$. Como el polinomio mínimo está determinado unívocamente, entonces $\bar{f}_r(x) = \bar{f}_s(x)$. Dado que φ es un isomorfismo, se tiene que $f_r(x) = f_s(x) = f(x)$. Como r y s son la k-sima raíz de $f(x)$, tenemos que $r = s$ y Φ es inyectiva.

- Sea $\bar{r}$ un elemento cualquiera de R_2 y $g(x)$ su polinomio mínimo sobre F_2. Supongamos que las raíces de $g(x)$ en R_2 están ordenadas y que $\bar{r}$ es su k-sima raíz. Dado que φ es sobreyectiva, existe $f(x) \in F_1[x]$, mónico e irreducible, de modo que $\bar{f}(x) = g(x)$. Por el Lema 3.5, $f(x)$ tiene el mismo número de raíces en R_1 que $g(x)$ en R_2. Por tanto, existe $r \in R_1$ raíz k-sima de $f(x)$ y se cumple que $\Phi(r) = \bar{r}$. Entonces, Φ es sobreyectiva.

Ahora vamos a probar que Φ es un homomorfismo. Sean r y s dos elementos de R_1. Tomamos como S el subconjunto formado por las raíces de los polinomios mínimos sobre F_1 de r, s, $r+s$ y rs. Aplicando el Lema 3.6, tenemos que existe un monomorfismo η que extiende a φ y conserva el orden de los elementos de S. Si u es cualquiera de los elementos de S y $f_u(x)$ su polinomio mínimo sobre F_1, $\eta(u)$ tiene que ser raíz de $\bar{f}_u(x)$, debido a que η es homomorfismo. Usando esto y que η conserva el orden de los elementos de S, se tiene que $\eta(r) = \Phi(r)$, $\eta(s) = \Phi(s)$, $\eta(r+s) = \Phi(r+s)$ y $\eta(rs) = \Phi(rs)$. Dado que η es homomorfismo, $\Phi(r+s) = \eta(r+s) = \eta(r)+\eta(s) = \Phi(r)+\Phi(s)$. Haciendo lo propio con rs, llegamos a que Φ es homomorfismo. Como también es biyectivo, Φ es un isomorfismo entre R_1 y R_2.

Para ver que Φ es un isomorfismo ordenado, tomamos un elemento positivo r de R_1. Dado que R_1 es real cerrado, existe $b \in R_1$ tal que $b^2 = r$. Por tanto, $\Phi(r) = \Phi(b^2) = \Phi(b)^2$ es un cuadrado no nulo de R_2. Entonces, Φ conserva el orden.

Por último, veamos que Φ es único. Supongamos que existe otro isomorfismo ordenado Φ' entre R_1 y R_2. Usamos lo mismo que hemos dicho antes, si $r \in R_1$ y $f_r(x)$ es su polinomio mínimo sobre F_1, entonces $\Phi'(r)$ tiene que ser raíz de $\bar{f}_r(x)$. Como hemos supuesto que Φ' también conserva el orden, no queda otra opción que $\Phi'(r) = \Phi(r)$. Por tanto, Φ es el único isomorfismo ordenado entre R_1 y R_2 que extiende a φ. □

Capítulo 4

Teorema de Artin-Schreier

En este último capítulo, vamos a dar una última caracterización de los cuerpos reales cerrados, que fue probada por Artin y Schreier:

Teorema 4.1 (Teorema de Artin-Schreier)**.** *Sea C un cuerpo algebraicamente cerrado. Si R es un subcuerpo propio de C con $[C : R]$ finito, entonces R es real cerrado y $C = R(i)$.*

Como se puede apreciar, las condiciones necesarias son mínimas; esto hace que el teorema sea realmente general. No está de más recalcar la condición de que R sea un subcuerpo *propio* de C. Si $R = C$, no sería posible que R sea real cerrado y algebraicamente cerrado a la vez ($i \in C$).

Además, no se descarta que, en un principio, el cuerpo tenga característica distinta de 0. Por esta razón, serán importantes los siguientes lemas sobre cuerpos de característica $p \neq 0$. Algunas demostraciones de estos resultados están remitidas a la bibliografía debido a que, o bien es necesario un estudio de cuerpos finitos que está fuera del objetivo de este trabajo, o bien, darían lugar a una transcripción literal de la bibliografía.

Lema 4.2. *Sea F un cuerpo de característica p. Si $f(x)$ es un polinomio irreducible de $F[x]$, se cumple:*

$$f'(x) = 0 \iff f(x) = a_0 + a_1 x^p + \ldots + a_l x^{lp}.$$

Lema 4.3 ([2], Lema 1 p. 655)**.** *Sea F un cuerpo de característica p. Si m es un elemento de F que no es p-potencia de F, entonces el polinomio $x^{p^e} - m$ es irreducible en $F[x]$, para cualquier $e \geq 1$.*

Teorema 4.4 ([2], Lema 2 p. 655)**.** *Sea F un cuerpo de característica $p \neq 0$ y $m \in F$. El polinomio $x^p - x - m$ es irreducible en $F[x]$ si y sólo si m no es de la forma $u^p - u$, $u \in F$.*

Lema 4.5 ([2], Lema 3 p. 655)**.** *Sea F un cuerpo de característica p y m un elemento de F que no es de la forma $u^p - u$, $u \in F$. Si E es un cuerpo de escisión de $x^p - x - m$ sobre F, entonces existe una extensión K de E tal que $[K : E] = p$.*

Definición 4.6. *Un cuerpo F se dice **perfecto** si toda extensión algebraica de F es separable.*

Para el siguiente resultado, es importante recordar que un polinomio irreducible $h(x)$ es separable si y sólo si $h'(x) \neq 0$.

Teorema 4.7. *Todo cuerpo de característica 0 es perfecto.*

Si F es un cuerpo de característica $p \neq 0$, F es un cuerpo perfecto si y sólo si todo elemento de F es p-potencia de F.

Demostración. Como bien sabemos, si un cuerpo tiene característica 0, toda extensión algebraica suya es separable. Por ello, todo cuerpo de característica 0 es perfecto.

Sea F un cuerpo perfecto de característica p. Si existe $m \in F$ que no es una p-potencia de F, por el Lema 4.3, $x^p - m$ es un polinomio irreducible de $F[x]$. Pero esto se contradice con el hecho de que F sea perfecto, porque $(x^p - m)' = px^{p-1} \equiv 0$ y $x^p - m$ no puede ser separable. Entonces, todo elemento de F es una p-potencia de F.

Ahora supongamos que F es un cuerpo de característica p y que todo elemento de F es una p-potencia de F. Sea $f(x) \in F[x]$ un polinomio irreducible. Si $f(x)$ no es separable, entonces $f'(x) = 0$. Por el Lema 4.2, $f(x) = a_0 + a_1x^p + \ldots + a_lx^{lp}$. Como cada elemento de F es una p-potencia, existen ciertos $b_i \in F$ de modo que $f(x) = b_0^p + b_1^p x^p + \ldots + b_l^p x^{lp}$. Entonces, $f(x) = (h(x))^p$, para cierto $h(x) \in F[x]$; pero esto es absurdo ya que habíamos supuesto que $f(x)$ es irreducible en $F[x]$. Por tanto, F es un cuerpo perfecto. □

Definición 4.8. *Una extensión F/K se dice **cíclica** si es una extensión de Galois y $Aut_K F$ es un grupo cíclico.*

Teorema 4.9 ([3], Proposición 7.8 p. 293)**.** *Sea K un cuerpo de característica p. F es una extensión cíclica sobre K de dimensión p si y sólo si F es cuerpo de escisión sobre K de un polinomio irreducible de la forma $x^p - x - m \in K[x]$. En este caso, $F = K(u)$ con u cualquier raíz de $x^p - x - m$.*

Teorema 4.10 ([3] Teorema 7.11 p. 295)**.** *Sea p un número primo y K un cuerpo que contiene a las distintas raíces p-simas de la unidad. Si F es una extensión cíclica sobre K de dimensión p, entonces $F = K(u)$ donde u es un elemento de F con polinomio mínimo sobre K de la forma $x^p - m \in K[x]$.*

Teorema 4.11 ([1], Teorema 4.21 p. 276)**.** *El grupo de Galois G del p^e-simo cuerpo ciclotómico sobre $\mathbb{Q}$, con p primo, es cíclico a menos que $p = 2$ y $e \geq 3$. En ese caso, G es un producto directo de un grupo cíclico de orden 2 y un grupo de orden 2^{e-2}.*

Teorema 4.12 ([1], Ejercicio 1 p. 256)**.** *Sea F un cuerpo y p un número primo que no es igual a la característica de F. Si $a \in F$, el polinomio $x^p - a$, o bien es irreducible en $F[x]$, o bien tiene una raíz en F.*

Demostración del Teorema 4.1. Supongamos que C es un cuerpo algebraicamente cerrado y R un subcuerpo propio verificando $[C : R] < \infty$. Consideremos $C' = R(\sqrt{-1})$, subcuerpo de C. Puesto que $C \supsetneq R$, si probamos que $C' = C$, obtendremos que $\sqrt{-1} \notin R$ y $R(\sqrt{-1}) = C$. Aplicando el Teorema 2.13, llegaríamos a que R es real cerrado.

Dado que C es algebraicamente cerrado, C es una clausura algebraica de R y C'. Además, como C es de dimensión finita sobre R, entonces C también es de dimensión finita sobre C'. Por otro lado, podemos ver que C' es un cuerpo perfecto. Si no fuese así, por el Teorema 4.7, la característica sería $p \neq 0$ y existiría un elemento m de C' que no sería p-potencia de F. Por el Lema 4.3, tenemos que para cada $e \geq 1$, el polinomio $x^{p^e} - m$ sería irreducible en $C'[x]$. Con ello, un cuerpo de escisión de este polinomio sobre C' sería una extensión de grado p^e sobre C', para cada $e \geq 1$. Pero esto no puede ocurrir debido a que $[C : C']$ es finito. Por tanto, C' es un cuerpo perfecto y C/C' es una extensión finita y separable.

Con esto, como C es una clausura algebraica de C', C/C' es una extensión de Galois. Sea G el grupo de Galois de esta extensión. Recordemos que queremos probar que $C' = C$; si esto no fuese así, entonces $|G| \neq 1$ y existe al menos un p primo tal que $p \mid |G|$. Por el Primer Teorema de Sylow (pág. 23), existe un subgrupo H de G tal que $|H| = p$. Si E es el cuerpo intermedio de C'/C fijado por H, C/E es de Galois y $[C : E] = p$.

Dado que C/E es de Galois, también es una extensión separable. Además, como $[C : E]$ es finito, aplicando el Teorema del Elemento Primitivo, C/E es una extensión simple. Dado que la dimensión es un número primo, para cualquier $z \in C \setminus E$, $C = E(z)$. Por la misma razón, los polinomios irreducibles de $E[x]$ sólo pueden tener grado 1 o p. Asimismo, como el grupo de Galois tiene orden primo, C/E es una extensión cíclica de dimensión p. Ahora vamos a usar los resultados expuestos antes sobre extensiones cíclicas.

Veamos que p no puede ser la característica. Si fuese así, por el Teorema 4.9, $C = E(u)$ para cierto $u \in C$ con polinomio mínimo sobre E de la forma $x^p - x - m$. Por el Lema 4.5, existe una extensión K de grado p sobre C. Pero esto es absurdo ya que C es algebraicamente cerrado. Entonces p no es la característica.

Ahora, vamos a aplicar el Teorema 4.10. Dado que C es algebraicamente cerrado, todas las raíces p-simas de la unidad se encuentran en C; estas son raíces del polinomio $x^p - 1 = (x - 1)(x^{p-1} + \ldots + 1)$. Como los polinomios irreducibles de $E[x]$ tienen grado 1 o p, $x^p - 1$ se escinde en E y todas las raíces p-simas de la unidad están contenidas en E. Por el Teorema 4.10, $C = E(u)$ para cierto $u \in C$ con polinomio mínimo sobre E de la forma $x^p - m$ ($m \neq 1$).

Consideremos el polinomio $x^{p^2} - m$. Las raíces de este polinomio son lo que conocemos como raíces p^2-simas de m. Estas se escriben de la forma: $l^i s$, con $1 \leq i \leq p^2$; donde l es una raíz primitiva p^2-sima de la unidad (existente debido a que la característica es distinta de p) y s es un elemento de C (algebraicamente cerrado) tal que $s^{p^2} = m$. Ninguna de estas raíces pertenece

a E, debido a que si $l^i s \in E$, entonces $(l^i s)^p \in E$; pero como $((l^i s)^p)^p = m$, se estaría contradiciendo el hecho de que $x^p - m$ es irreducible en $E[x]$. Por tanto, ninguna de las raíces de $x^{p^2} - m$ pertenece a E y su factorización en irreducibles de $E[x]$ consiste en p polinomios de grado p.

El término independiente de cualquiera de los factores irreducibles de $x^{p^2} - m$ tiene que ser de la forma $b = vs^p$, con v una potencia de l ($v \neq 1$ debido a que l es una raíz *primitiva* p^2-sima de la unidad). Razonando como antes, debido a que $(s^p)^p = m$, s^p y s^{-p} no pertenecen a E. Puesto que b sí pertenece a E (por ser coeficiente de un polinomio de $E[x]$), se tiene que $bs^{-p} = v$ tampoco pertenece a E. Por otra parte, como l es una raíz primitiva p^2-sima y v es una potencia de l, se cumple que $v^{p^2} = 1$. Entonces el orden de v es divisor de p^2. Como E contiene a todas las raíces p-simas de la unidad y $v \notin E$, sólo es posible que el orden de v sea p^2 y, por tanto, v es una raíz primitiva p^2-sima de la unidad. Con esto, E no contiene ninguna raíz primitiva p^2-sima de la unidad.

Por otro lado, llamemos P al cuerpo primo de C y consideremos el cuerpo $P(v)$. Si F es el p^k-simo cuerpo ciclotómico sobre P, por los resultados conocidos de un cuerpo ciclotómico, la dimensión de F sobre P tiende a infinito si también lo hace k. En cambio, como $[P(v) : P]$ es divisor de $\varphi(p^2)$, esta otra dimensión es finita. Por ello, ha de existir r (fijo) tal que $P(v)$ contiene una raíz primitiva p^r-sima de la unidad, pero ninguna raíz primitiva p^{r+1}-sima de la unidad. Dado que v es una raíz primitiva p^2-sima de la unidad, este r es mayor o igual que 2.

Sea $w \in C$ una raíz primitiva p^{r+1}-sima de la unidad (de nuevo existente debido a que la característica es distinta de p). Dado que E no contiene ninguna raíz primitiva p^2-sima de la unidad, tampoco contiene ninguna raíz primitiva p^t-sima, para todo $t \geq 2$. En particular, $w \notin E$ y $C = E(w)$. Con esto, el polinomio mínimo de w sobre E tiene grado p. Como $P \subseteq E$, w tampoco pertenece a P y $[P(w) : P] \geq p$.

Como la característica es distinta de p y w es una raíz primitiva p^{r+1}-sima de la unidad, $P(w)$ es un cuerpo ciclotómico sobre P; y por tanto, es de Galois sobre el mismo. Si $K = Aut_P P(w)$, entonces $|K| \mid \varphi(p^{r+1}) = p^r(p-1)$. Como $[P(w) : P] \geq p$, $|K|$ tiene al menos p elementos; por tanto, $|K| \nmid (p-1)$. Si la característica es positiva, K es cíclico debido a que $P(w)$ es una extensión finita de P. Si la característica es 0, K es isomorfo a $U(\mathbb{Z}/p^{r+1}\mathbb{Z})$; y por el Teorema 4.11, K es cíclico a no ser que $p = 2$ y $r \geq 2$. Supongamos que estamos en los casos en que K es cíclico. Como $|K| \mid p^r$, ha de contener un único subgrupo de orden p. Por la biyección en el Teorema Fundamental de la Teoría de Galois, existe un único cuerpo intermedio M de $P(w)/P$ de modo que $[P(w) : M] = p$. En lo que queda de demostración, vamos a ver que, en este caso, $P(w)$ tiene dos subcuerpos distintos sobre los que tiene dimensión p. Con esto, tan sólo nos quedaría la opción de que la característica es 0 y $p = 2$.

Habíamos visto que $w \notin E$. Si $h(x)$ es el polinomio mínimo de w sobre E, entonces el grado de $h(x)$ es p. Además, $h(x)$ es divisor de $x^{p^{r+1}} - 1$ debido a

que w se anula en él. De la misma forma que antes, la factorización completa de este polinomio es de la forma: $\prod_{i=1}^{p^{r+1}} (x - w^i)$. Por tanto, $h(x)$ ($\in E[x]$) también pertenece a $P(w)[x]$. Si D es el cuerpo intersección $E \cap P(w)$, entonces $h(x)$ es irreducible en $D[x]$ (por serlo en $E[x]$). Con esto, el polinomio mínimo de w sobre D también es $h(x)$. Por tanto, $[P(w) : D] = p$.

Tomemos ahora $z = w^p \in P(w)$. Como es una raíz (primitiva) p^r-sima de la unidad, $z \in P(v)$ por como hemos elegido r. Consideremos el subcuerpo $P(z) \subseteq P(w)$. Por el Teorema 4.12, el polinomio $x^p - z \in P(z)[x]$, o bien es irreducible, o bien tiene una raíz en $P(z)$. Supongamos que estamos en el segundo caso. Como z es una raíz primitiva p^r-sima de la unidad, $P(z)$ también contiene a una raíz primitiva p-sima de la unidad. Esto sumado a que hemos supuesto que $P(z)$ contiene una raíz de $x^p - z$, tenemos que este polinomio tiene todas sus raíces en $P(z)$. Como w es raíz de $x^p - z$, $w \in P(z)$ y entonces $P(z) = P(w)$. Con esto, como $P(v)$ contiene a z, también tendría que contener a w. Pero esto es absurdo, debido a que $P(v)$ no contiene ninguna raíz primitiva p^{r+1}-sima. Por tanto, sólo es posible que $x^p - z$ sea irreducible en $P(z)[x]$. Con esto, $x^p - z$ es el polinomio mínimo de w sobre $P(z)$, y entonces $[P(w) : P(z)] = p$.

Por último veamos que los cuerpos D y $P(z)$ son distintos. Si no lo fuesen, z pertenecería a $D = E \cap P(w)$. Entonces, E contendría una raíz primitiva p^r-sima de la unidad. Pero esto no es posible por lo que hemos dicho antes (E ni siquiera contiene una raíz primitiva p^2-sima de la unidad).

Entonces, hemos encontrado dos subcuerpos distintos de $P(w)$, D y $P(z)$, sobre los que tiene dimensión p. Como habíamos dicho antes, esto contradice al hecho de que $P(w)/P$ sea de Galois. Por tanto, tan sólo nos queda como único caso posible que la característica sea 0 y $p = 2$. Entonces $[C : E] = 2$ y v es una raíz primitiva 2^2-sima de la unidad, es decir, $v = \pm\sqrt{-1}$. Pero todo esto es absurdo, porque según como hemos construido E, $\sqrt{-1} \in E$. Entonces, no se cumple que $v \notin E$, ni tampoco que $[C : E] = 2$. En consecuencia, no es posible que $C' \neq C$ y la demostración estaría acabada. □

Apéndice A

Primer Teorema de Sylow

Para poder probar el Primer Teorema de Sylow, es necesario introducir ciertos términos acerca de acción de grupo y grupos finitos.

Definición A.1. *Dado un conjunto S y un grupo G, una acción a izquierda del grupo G sobre S es una aplicación:*

$$\begin{aligned} \cdot_G : G \times S &\longrightarrow S \\ (g, x) &\longmapsto gx \end{aligned}$$

cumpliendo:

1. *Para cualesquiera g_1, $g_2 \in G$ y $x \in S$, $g_1(g_2x) = (g_1g_2)x$.*
2. *Si e es el elemento neutro de G, $ex = x$ para todo $x \in S$.*

Ejemplo A.2. *Sea G un grupo y H un subgrupo de G. Si $h \in H$ y K es cualquier subgrupo de G, entonces $hKh^{-1} = \{hkh^{-1} : k \in K\}$ también es subgrupo de G ($e = heh^{-1} \in hKh^{-1}$, $(hkh^{-1})^{-1} = hk^{-1}h^{-1} \in hKh^{-1}$). Si tomamos como S al conjunto de los subgrupos de G, podemos definir la siguiente aplicación:*

$$\begin{aligned} H \times S &\longrightarrow S \\ (H, K) &\longmapsto hKh^{-1} \end{aligned}$$

es fácil comprobar que es una acción debido a que $eKe^{-1} = K$ y $h_1h_2Kh_2^{-1}h_1^{-1} = (h_1h_2)K(h_1h_2)^{-1}$, para cualesquiera $K \in S$ y h, h_1, $h_2 \in H$.

Sea G un grupo que actúa sobre un conjunto S. Si $gx = y$, para ciertos $g \in G$ y $x \in S$, entonces $g^{-1}y = g^{-1}gx = ex = x$.

Por otra parte, para cada $x \in S$, denotemos por G_x al subconjunto de elementos g de G tales que $gx = x$. Comúnmente, este subconjunto se conoce por **estabilizador de** x. El elemento neutro e pertenece a G_x por definición de acción de grupo. Además, si $g \in G_x$, como $x = gx$, también se cumple que $g^{-1}x = g^{-1}gx = ex = x$. Por tanto, $g^{-1}x = x$ y $g^{-1} \in G_x$. Con esto, se cumple lo siguiente:

Proposición A.3. *Sea G un grupo que actúa sobre un conjunto S. Para cada $x \in S$, el conjunto $G_x = \{g \in G : gx = x\}$ es un subgrupo de G.*

Ejemplo A.4. *Si consideramos la acción de grupo del ejemplo anterior, para cada subgrupo $K \in S$, el conjunto $H_K = \{h \in H : hKh^{-1} = K\}$ lo denotaremos por $N_H(K)$ y lo llamaremos* ***normalizador de*** *K* ***en*** *H. Si la acción está aplicada por $H = G$, al subgrupo $N_G(K)$ tan sólo lo llamaremos* ***normalizador de*** *K.*

Está claro que $K \subseteq N_G(K)$, debido a que $kKk^{-1} = K$ para cualquier $k \in K$. Además, como $hKh^{-1} \subseteq K$ para cualquier $h \in N_G(K)$, entonces se tiene que K es un subgrupo normal de $N_G(K)$.

Definición A.5. *Si G es un grupo que actúa sobre un conjunto S y x un elemento de S, llamaremos* ***órbita de x*** *al conjunto $orb(x) = \{gx : g \in G\}$.*

Proposición A.6. *Siguiendo con la notación de la definición anterior, el cardinal del conjunto $orb(x)$ es el mismo que el índice $|G : G_x|$.*

Demostración. Si $y \in orb(x)$, existe $g \in G$ tal que $gx = y$. Podemos establecer una biyección entre el conjunto $orb(x)$ y el conjunto de las clases a izquierda de G_x en G, dada de la forma: $gx \longmapsto gG_x$. Esta aplicación está bien definida debido a que $g \in G$; también es sobreyectiva porque para todo $g \in G$, $gx \in orb(x)$. Para ver que es inyectiva, basta con darse cuenta de:

$$g_1G_x = g_2G_x \Leftrightarrow {g_2}^{-1}g_1 \in G_x \Leftrightarrow {g_2}^{-1}g_1x = x \Leftrightarrow g_1x = g_2x.$$

□

Por último, si G es un grupo que actúa sobre un conjunto S, el subconjunto $S_0 = \{x \in S : gx = x \ \forall g \in G\}$ lo denominaremos **subconjunto de S fijado por G**. Ahora, ya podemos introducir los siguientes resultados:

Lema A.7. *Si G es un grupo finito de orden p^n (p primo) que actúa sobre un conjunto finito S, entonces $|S| \equiv |S_0|$ mód. p.*

Demostración. Si $x \in S_0$, entonces $|orb(x)| = 1$. Por tanto, podemos escribir S como unión disjunta $S_0 \cup orb(x_1) \cup orb(x_2) \cup \ldots \cup orb(x_n)$, donde $|orb(x_i)| > 1$ para todo i. Entonces, $|S| = |S_0| + |orb(x_1)| + \ldots + |orb(x_n)|$.

Por lo visto en la Proposición A.6, para cada i, $|orb(x_i)| = |G : G_{x_i}|$. Como $|G| = p^n$, $p \mid |orb(x_i)|$, para cada i. Por tanto, $|S| \equiv |S_0|$ mód. p. □

Teorema A.8 (Teorema de Cauchy)**.** *Sea G un grupo finito con $|G| = n$ y p un número primo divisor de n, entonces G contiene un elemento de orden p.*

Demostración. Sea $S = \{(a_1, a_2, \ldots, a_p) : a_i \in G \wedge a_1a_2 \cdots a_p = e\} \subseteq G^p$. Como para cada p-tupla, el elemento a_p queda determinado por $(a_1a_2 \cdots a_{p-1})^{-1}$, el cardinal de S es $|G|^{p-1} = n^{p-1}$.

Ahora vamos a definir una acción del grupo $\mathbb{Z}/p\mathbb{Z}$ sobre el conjunto S:

$$(k, (a_1, a_2, \ldots, a_p)) \mapsto (a_{k+1}, a_{p+2}, \ldots, a_p, a_1, \ldots a_k).$$

Se puede comprobar que esta aplicación está bien definida y que es una acción de grupo mediante las propiedades de $\mathbb{Z}/p\mathbb{Z}$. Como $|\mathbb{Z}/p\mathbb{Z}| = p$, aplicando el Lema A.7, $|S| \equiv |S_0|$ mód. p, donde S_0 es el subconjunto de S fijado por $\mathbb{Z}/p\mathbb{Z}$. Dado que $p \mid |S|$, $|S_0| \equiv 0$ mód. p.

Por la definición de S_0, todos sus elementos son de la forma $(a_1, a_2, \ldots, a_p)$ con $a_1 = a_2 = \ldots = a_p$. Un elemento que seguro que estará en S_0 es $(e, e, \ldots, e)$, con lo que $|S_0| \neq 0$. Por ello, S_0 contiene al menos p elementos distintos. Así, existe $a \in S$ tal que $a^p = e$ (p divide el orden de a). Como p es primo, el orden de a es p. □

Definición A.9. *Diremos que un grupo finito G es un **p-grupo** (p un número primo) si el orden de cada elemento de G es una potencia de p. Un subgrupo de un grupo cualquiera se llama **p-subgrupo** si es un p-grupo.*

Ahora se darán dos lemas muy útiles para la demostración del Primer Teorema de Sylow. No serán dadas las demostraciones debido a que son muy sencillas.

Lema A.10. *Un grupo finito G es un p-grupo si y sólo si $|G|$ es una potencia de p.*

Lema A.11. *Si G es un grupo finito y H un p-subgrupo de G de modo que $p \mid |G/H|$, entonces p divide a $|N_G(H)/H|$.*

Teorema A.12 (Primer Teorema de Sylow)**.** *Sea G un grupo finito de orden $p^n m$, con p primo, $n \geq 1$ y $(p, m) = 1$. Existe un subgrupo de G de orden p^i, para cada $1 \leq i \leq n$. Además, todo subgrupo de G de orden p^i ($i < n$) es normal en algún otro subgrupo de orden p^{i+1}.*

Demostración. Podemos probar este resultado mediante inducción. Dado que $p \mid |G|$, por el Teorema A.8, G contiene un elemento a de orden p. Considerando el subgrupo generado por a, tenemos el primer caso, un subgrupo de orden p.

Como hipótesis de inducción, supongamos que existe un subgrupo H de orden p^i ($|G/H| = p^{n-i}m$) para cada $i < n$. Hemos de encontrar un subgrupo de orden p^{i+1}. Además, se pedirá que H sea normal (que esté contenido también) en este nuevo subgrupo, para cumplir la segunda parte del enunciado del teorema. Por los lemas anteriores, H es un p-subgrupo y p divide a $|N_G(H)/H|$. Dado que H es un subgrupo normal normal de $N_G(H)$, $N_G(H)/H$ es un grupo cociente. Al igual que en el caso inicial, $N_G(H)/H$ contiene un subgrupo de orden p.

El subgrupo encontrado, por ser subgrupo de un grupo cociente, es de la forma J/H, con J un subgrupo de $N_G(H)$ conteniendo a H. Por el Teorema de Lagrange, se tiene que $|J| = |J/H||H|$; por tanto, $|J| = p^{i+1}$. Además, como H es normal en $N_G(H)$, se ha de cumplir que H también es normal en J. □

Bibliografía

[1] Nathan Jacobson, *Basic Algebra I*, W. H. Freeman and Company, New York, 1985.

[2] Nathan Jacobson, *Basic Algebra II*, W. H. Freeman and Company, New York, 1980.

[3] Thomas W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.

[4] Saugata Basu, Richard Pollack and Marie-Françoise Roy, *Algorithms in Real Algebraic Geometry*, Springer-Verlag, Berlin, Heidelberg, 2003.

[5] Serge Lang, *Algebra*, Addison-Wesley, 1965.

[6] Cortaduras de Dedekind, http://www.esacademic.com/dic.nsf/eswiki/307120, diciembre 2018.